BB

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-124996
(43)Date of publication of application : 26.04.2002

(51)Int.Cl. H04L 12/66
G06F 13/00

(21)Application number : 2000-350265
(22)Date of filing : 13.10.2000

(71)Applicant : BABA YOSHIMI
(72)Inventor : BABA YOSHIMI

## (54) FAST PACKET ACQUIRING ENGINE/SECURITY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a cracker monitor system of a simple system configuration to protect an LAN 1 from attacking by a cracker by automatically detecting the attack by the cracker to the LAN 1 with no burdensome limit on communication or experienced engineers.
SOLUTION: A sensor 5 is provided where a hash algorithm is used to sequentially acquire IP packets passing an entrance of a LAN 1. The sensor 5 quickly detects various attacks by a cracker to the LAN 1 based on the acquired IP packet. The information related to the attack which is detected by the sensor 5 is provided to a director 6 controlling a fire wall 2. The director 6 controls setting of the fire wall 2 according to the supplied information and prevents an IP packet related to the detected attack from entering the LAN 1.

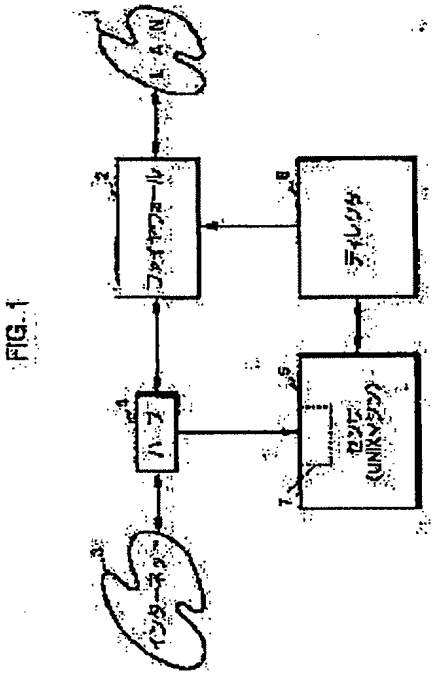


FIG. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－124996
（Ｐ2002－124996Ａ）
(43)公開日　平成14年４月26日(2002.4.26)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ　12/66 | | Ｈ０４Ｌ　12/66 | Ｂ | ５Ｂ０８９ |
| Ｇ０６Ｆ　13/00 | ３５１ | Ｇ０６Ｆ　13/00 | ３５１Ｚ | ５Ｋ０３０ |

審査請求　未請求　請求項の数６　書面　（全 14 頁）

(21)出願番号　特願2000－350265(Ｐ2000－350265)

(22)出願日　平成12年10月13日(2000.10.13)

(71)出願人　599098415
馬場　芳美
横浜市港北区太尾町644
(72)発明者　馬場　芳美
神奈川県横浜市港北区太尾町644

Ｆターム(参考)　5Ｂ089 ＧＡ04 ＨＡ04 ＨＡ10 ＨＢ02 ＫＣ18
ＫＨ28 ＭＣ08
5Ｋ030 ＧＡ14 ＨＡ08 ＨＣ01 ＨＣ14 ＨＤ03
ＨＤ06 ＪＡ10 ＫＡ06 ＫＡ13 ＬＣ14
ＬＣ15 ＬＣ16 ＭＡ04 ＭＢ18

(54)【発明の名称】　高速パケット取得エンジン・セキュリティ

(57)【要約】
【課題】ＬＡＮ１に対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するＬＡＮ１の保護を図ることができるクラッカー監視システムである。
【解決手段】ハッシュアルゴリズムを用いる事で、ＬＡＮ１の入り口にそこを通るＩＰパケットを逐次取得するセンサ５を設ける。センサ５は、取得したＩＰパケットに基づき、ＬＡＮ１に対するクラッカーからの各種攻撃を高速に検知する。センサ５が検知した攻撃に関する情報は、ファイヤウォール２を制御するディレクタ６に与えらる。ディレクタ６は与えられた情報に応じてファイヤウォール２の設定を制御し、検知された攻撃に係るＩＰパケットがＬＡＮ１に進入するのを阻止する。

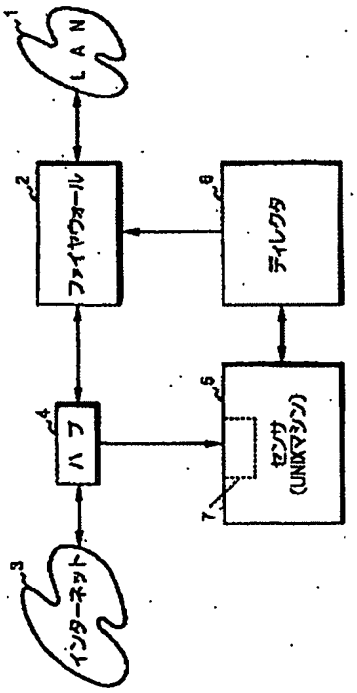



FIG. 1

【特許請求の範囲】
【請求項１】ネットワークを高速に流れるパケットを通過させる機器に於いて、そのパケットを遅滞なく通過させる時間内に、それを検出分類し、適切な処理を施す事が出来る事に特徴を有する、通信用装置。
【請求項２】送信および受信情報をハッシュ法によって圧縮し、充分狭いメモリー空間内に全情報を展開する事を可能とした事に特徴を有する、上記、請求項１に記載の通信用装置。
【請求項３】ハッシュ表作製時に、２重ハッシュとリスト方式を利用する事により、高効率を達成する事に特徴を有する、上記、請求項１及び／乃至は２に記載の通信用装置。
【請求項４】ハッシュ表利用時に圧縮率を制御し、メモリー利用率を約８０％に保つ事で、衝突を避けつつ、高効率を達成する事に特徴を有する、上記、請求項１及び／乃至は２及び／乃至は３に記載の通信用装置。
【請求項５】インターネット上のハッキング乃至はクラッキングと言われる攻撃、特に、ＴＣＰ－Ｓｙｎ Ｆｌｏｏｄ、Ｔｅａｄｒｏｐ、Ｌａｎｄ、Ｐｉｎｇｏｆ Ｄｅａｔｈ、Ｄｉｓｔｒｉｂｕｔｅｄ Ｄｅｎｉａｌ ｏｆ Ｓｅｒｖｉｃｅを、検出及び／乃至は遮断する事を目的とした上記、請求項１及び／乃至は２及び／乃至は３及び／乃至は４に記載の通信用安全装置。
【請求項６】インターネット上の通信を利用して、ＯＳのバグ等のバッファーオーバーフローを起こさせるなどして、ルートのパスワードを奪取するなどの攻撃が起こった時に、高速にそれに関する通信データを補足する事に特徴を有する上記、請求項１及び／乃至は２及び／乃至は３及び／乃至は４及び／乃至は５に記載の通信用安全装置。
【発明の詳細な説明】
【００１】
【発明の属する技術分野】　本発明は、クラッカーによるインターネットを介したネットワーク（ＬＡＮ）への攻撃を監視し、さらにはその攻撃からネットワークを保護するためのシステムに関する。
【従来の技術】　近年、企業などの組織内に構築されたネットワーク（ＬＡＮ）は、その多くがインターネットに接続され、他のネットワーク等との間での各種情報のやりとり（通信）がインターネットを介して行われている。この通信では、一般に、所謂ＯＳＩ階層モデルにおけるネットワーク層に主として対応するプロトコルとしてＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）が用いられ、通信データはＩＰパケットの形態でやりとりされる。そして、上記ネットワーク層の上位のトランスポート層に主として対応するプロトコル（ＩＰの上位のプロトコル）として、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）あるいはＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）を用いるのが通例である。
【００２】この種のネットワークは、インターネット上のサーバや他のネットワークなどとの間で、多種多様な情報のやりとりを低コストで行うことができるという利点を有する。反面、インターネットが極めて高度な公開性を有することから、所謂クラッカーからの攻撃を受ける危険性にさらされることとなる。このため、そのような攻撃からネットワークを保護することが要求される。このようなネットワークの保護を行うためのシステムとしては、従来、保護しようとするネットワークの入り口に、ファイヤウォール（詳しくはファイヤウォールの機能をもたせたコンピュータ）を設けたシステムが知られている。このファイヤウォールは、あらかじめネットワーク管理者などが定めた種類の通信がネットワーク内とその外部との間で行われるのを阻止し、それ以外の許可された通信のみをネットワーク内とその外部との間で行うことができるようにするものである。この場合、阻止する通信の種類は、例えばＩＰパケットに含まれる送信元ＩＰアドレスや宛先ＩＰアドレス、宛先ポート番号などによって指定可能とされている。このようなファイヤウォールによれば、ネットワーク内の特定のＩＰアドレスを有するホスト（コンピュータ）、あるいはそのホストの特定のポート番号に対する外部からのアクセスを禁止したり、ネットワークの外部の特定のＩＰアドレス以外のＩＰアドレスからのネットワークへのアクセスを禁止したりすることができる。従って、ネットワークへの進入を禁止する通信データの種類をファイヤウォールに対して適切に設定しておけば、ネットワークへの攻撃の危険性を低減することが可能である。
【００３】更にこのようなネットワークへの攻撃を検出するためのシステムとしては、従来、保護しようとするネットワークの入り口に、侵入検知システム（英語ではｉｎｔｒｕｓｉｏｎ ｄｅｔｅｃｔｉｏｎ ｓｙｓｔｅｍ、詳しくは侵入者の通信パターンを検出する機能をもたせたコンピュータ）を設けたシステムが知られている。この侵入検知システムは、あらかじめ収集された種類の攻撃者に特有のパターンの通信がネットワーク内とその外部との間で行われるのを検出し、それを管理者に通報するものである。ここで、その検出には、データの収集およびデータベースの参照等の時間を要する為、攻撃が行われた事の検出に基づいてそれを遮断する、或いは、それ以外の許可された通信のみをネットワーク内とその外部との間で行うことができるようにするのは、通常不可能である。この場合、通信を阻止する為には、例えばＩＰパケットが通過するまでのかなり短時間の間に、通信に含まれる情報などによって検出特定が可能とされなくてはならない為、通常のパケット確認用のツールであるスニファー（ｓｎｉｆｆｅｒ）あるいはＢＰＦ（Ｂａｋｌｅｙ Ｐａｃｋｅｔ Ｆｉｌｔｅｒ）などでは遅すぎる。このように、ファイヤウォールによっても

侵入検知システムによっても、ネットワーク内とネットワークの外部で、ネットワークへの侵入を禁止する事は、適切に設定しておいても、ネットワークへの攻撃の危険性を減らすことはできても、なくすことは不可能である。つまり、ファイヤウォールや侵入検知システムにより防御するには、保護しようとするネットワーク内の各ホストがどのような情報を利用し、もしくは外部に提供し、また、ネットワーク内のどのような情報を保護すべきか、予想される攻撃としてどのようなものが想定されるか、ということなどを総合的に考慮して決定しなければならないし、かなりな熟練技術者によっても場合によっては不可能な事情があった。

【００４】従って、ネットワークの管理運営には、常時、攻撃される事を前提とした修復を伴う、熟練技術者による多大な労力やコストを要するものとなっていた。また、上記のような従来のファイヤウォールは、攻撃の可能性のある通信をすべて排除しようとするものである。従って、設定により禁止された種類の通信は、その通信がクラッカーからの攻撃によるものであるか否かにかかわらず一律的に排除される。つまり、ネットワークと外部との通信の自由度が必要以上に制限される。このため、ファイヤウォールを備えたネットワークでは、インターネット上の利用可能な情報提供サービスの制限を受ける。この結果、インターネット上の多くの情報資源を有用に享受することができないという不都合を生じるものであった。

【００５】

【発明が解決しようとする課題】　本発明はかかる背景に鑑みてなされたものであり、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視攻撃遮断システムを提供することを目的とする。

【課題を解決するための手段】　本発明のクラッカー監視システムは、かかる目的を達成するために、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得して累積的に保持し、保持した複数のＩＰパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするものである。

【００６】すなわち、本願発明者等がクラッカーによる各種攻撃の手法を検討したところ、一般に、多くの種類の攻撃は、それぞれその攻撃の際に時系列的に通信される複数のＩＰパケットに特徴的な相互関連性を有する。従って、前記ネットワークの入り口で、そこを通過するＩＰパケットを前記攻撃検知手段によって逐次取得して累積的に保持し、その保持した複数のＩＰパケットを監視することで、クラッカーによる前記ネットワークへの攻撃をリアルタイムで検知することができる。そして、このように攻撃を検知できれば、それに応じて前記処理手段により適当な処理（例えばネットワーク管理者などへの報知や、クラッカーによる通信を遮断する処理等）を行うことで、その攻撃からのネットワークの保護を図ることができる。この場合、クラッカーによる攻撃を十分精度よく検知防御する為には、一般にかなりの高速度を要するに進行する。このため、攻撃を検知するために、高速度にＩＰパケットに関する情報を蓄積して行くテクニックとして、ハッシュ表のアルゴリズムを要する。あるいは、それによってネットワークを保護するための処置を行えば、ネットワークの損害を十分に抑えることができる。

【００７】このような本発明のシステムによれば、クラッカーによる攻撃をリアルタイムで検知できるので、その検知がなされたとき、且つそのときにのみ攻撃に対する対策処置を施せばよい。このため、ネットワーク管理者等は、所謂ログファイル（通信記録簿）等を頻繁に参照したりする必要性が低減される。さらに、ネットワークの構築や再編等の際に、クラッカーによる攻撃を予測的に考慮するような労力が軽減される。また、攻撃が検知されない通常時は、ネットワークとその外部との通信を、攻撃の可能性を予測して制限する必要性がなく、その通信の自由度を高めることができる。従って、本発明によれば、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができる。かかる本発明においては、前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのＩＰパケットを受信可能に構成しておく。これにより、クラッカーによる多くの種類の攻撃を速やかに検知することが可能となる。さらに、本発明では、前記攻撃検知手段は、ＩＰパケットの受信のみが可能に構成しておく。

【００８】これによれば、前記攻撃検知手段は、自己のＩＰアドレスやＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス等、自己情報のデータをネットワークに送信することがないため、クラッカーなどによりその存在が認識されたり、攻撃の対象とされることがない。従って、攻撃検知手段の安全性を確保し、ひいては、本発明のシステムの信頼性を確保することができる。また、本発明では、前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得して保持した前記複数のＩＰパケットから前記アルゴリズムに基づき各種類の攻撃を検知する。これにより、クラッカーによる複数の種類の攻撃を検知することが可能となり、前記ネット

ワークの安全性を高めることができる。また、前記アルゴリズムを適宜更新することで、新しい種類の攻撃に対しても対応することが可能となる。この場合、前記攻撃検知手段は、取得して保持した複数のＩＰパケットを少なくとも送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類する手段として、二重型リスト・ハッシュ方式を具備し、その分類した複数のＩＰパケットの為に表から前記各種類の攻撃を検知する。

【００９】すなわち、複数の種類の攻撃を検知するためには、ＩＰパケットの送信元ＩＰアドレスや宛先ＩＰアドレス（これらはＩＰパケットのＩＰヘッダに付与されている）が重要な鍵となることが多い。従って、所定時間内に取得したＩＰパケットを送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類して保持することで、それらのＩＰパケットから攻撃を検知しやすくなる。本発明では、より具体的には、前記攻撃検知手段は、次のようにハッシュ表によって攻撃を検知する。ハッシュ法（ｈａｓｈｉｎｇ）は、メモリ上でデータを高速に検索するための手法である。各種のツリー構造とは異なり、静的な配列だけで簡単に実装でき、効率も極めて高い。配列上でデータを検索する手法は、いくつかある。以下、単純な手法から順に説明していき、ハッシュ法の説明に至る。ある情報をメモリ上で処理する場合を考えてみよう。情報のキーとして番号（整数）を用いることだけを決めておき、その他については考えないことにする。

（１）単純配列

データの出現順に配列につめていく。もっとも単純かつ基本的な方法。データの挿入は高速だが、検索は端から順に見ていく（リニアサーチという）しかないため、平均するとデータ件数の半分について処理が必要となる。この手法は遅いので、データ件数が多い場合には使われない・・・と良いのだが、多くのプログラマがこの方法しか知らないが故に、現実には件数が多い場合にも使われている。

（２）ソート済み配列

あらかじめ配列上のデータをキー（この場合は社員番号）の順に整列しておく。こうすると、データの挿入には時間がかかる（後述）が、検索にバイナリサーチという手法が使えるので、高々ｌｏｇ（Ｎ）回の処理ですむ。１００万件のデータでもｌｏｇ（Ｎ）≒２０だから膨大なデータでも非常に高速である。一方、データの維持にはコスト（処理時間）がかかる。データの内容が固定的なもの（例：Ｖｉｓｕａｌ　Ｂａｓｉｃのキーワード…ｐｒｉｎｔなど）である場合や、データが発生するフェーズと参照されるフェーズがはっきり分れている場合（ＤＸＦの線種や複合図形定義）には、データをまとめてソートできるから、クイックソートなどの高速アルゴリズムを使用すればＮ＊ｌｏｇ（Ｎ）の手間である。これは各種のツリー構造と遜色ない。しかし、データをためつつ使用する場合は、ソート済みの配列にデータを挿入するしかなく、処理時間はＮの二乗のオーダーを要する、つまり遅い。

（３）逆引き表

小さなデータという前提なので、特殊なケースとして、番号が３桁の整数である場合を考えてみよう。この場合、番号は００１～９９９の１０００種類弱しかない。このため、あらかじめ１０００要素の配列を用意しておき、番号をインデックスとして配列に入れてしまうという方法がある。これを逆引き表という。情報をいれる場合の擬似コードは以下のようになる。

マスター［番号］＝内容

逆引き表の利点は、登録も検索も極めて高速であり、処理も単純なことである。一方欠点は、キーの範囲が小さくないと使えないことである。例えば、大きいデータでは番号は９桁以上だから１０億通りの可能性があり、逆引き表は現実的でない。このため、逆引き表はあまり一般的ではない。

（４）ハッシュ表

前述のように大きいデータの番号は９桁だが、数は１０００人そこそこである。このため、番号を適当な関数で０～１０００（現実には余裕を見て１２００くらいにとる）に写像できれば、逆引き表が使える。これをハッシュ関数といい、ハッシュ関数を使った逆引き表をハッシュ表という。簡単なハッシュ関数としては、番号を配列のサイズで割り算した余り、というのがある。今、配列のサイズを１２０１とすると、

ｈ（ｎ）＝ｎ　ｍｏｄ　１０２１　（ｍｏｄは剰余を求める演算子）

マスター［ｈ（番号）］＝内容

とすればよい理屈だが、一つ問題がある。一例として、番号は８５０６０４０１４であり、１０２１で割った余りは７４６だが、他にも余り（ハッシュ値）が７４６がいるかもしれない。これを衝突（ｃｏｌｌｉｓｉｏｎ：コリジョン）という。衝突があった場合の処理にはいろいろあるが、単純な対処としては、隣の欄を用いていく方法などがある。ハッシュ法は登録・検索とも極めて効率がよく、データ量が増えても検索の手間が変わらないという際立った特徴がある。にも関わらずハッシュ法が実務ではあまり使用されないのは、ハッシュ法を知らない人が多いし、メモリ上のハッシュは簡単だが、ディスクファイル上では手間が掛かる、などの理由が想起される。上記のハッシュ関数は非常に単純だが、文字列（例えば氏名）によるハッシュ関数にはもう少し工夫が必要である。文字列のハッシュとして以下のような関数を用いている。

ｈ＝（．．．（（ｓ［1］＊３７＋ｓ［2］）＊３７＋ｓ［3］）＊３７．．．）ｓ［ｎ］）＊３７

ハッシュ関数は、キーの値から「でたらめな値」を作り出す関数なので、乱数生成のアルゴリズムと関連があ

る。上記は「線形合同法」という乱数生成法と良く似ている。他の著名な乱数生成法の中では「平方採中法」もハッシュ関数として利用できる。また、ハッシュ関数は、元の値からできるだけ重複しない値を作り出すわけだから、データの特徴を示す「電子指紋」としてハッシュ関数と類似の関数が使用されるケースがある。この場合は関数の値域を十分大きくし、関数を工夫することにより、現実のデータではまず重複の起り得ない関数が工夫されている。電子指紋は、データが改竄（かいざん）されていないことを示す場合などに使用されており、電子商取引などに重要である。さらに、ハッシュ関数は元のデータからでたらめな値を作り出すことから、一種の暗号化のことをハッシュと呼ぶ場合があり、ハッシュという語感にはぴったりくるが、これは不正確な用法である。１２０１は素数である。表のサイズは素数が好ましい。性能は表の利用率によって異なる。利用率８割の場合、もっとも素朴な方法でも平均３回くらいの操作で検索可能である。ハッシュ表はデータが詰まってくると効率が悪くなるので、ある程度詰まってきたら（例：利用率９０%）、表のサイズを大きくしてデータを詰め直すこともある。これを再ハッシュ（ｒｅｈａｓｈ）という。ハッシュ（ｈａｓｈ）は英語で「切り刻む」という意味があり、ｈａｓｈｅｄ　ｂｅｅｆからハヤシライスの語源となった。

【０１０】検索という操作はプログラミングにおいて非常に頻繁に使われるもので、対象となるデータ量が比較的少ない場合には単純に順番に調べても最近の高速なマシンでは問題無い速度が得られるが、データ量が大きくなってきたり、頻繁に検索する必要がある場合に速度は非常に重要である。検索に関しては非常に多くの文献があり、詳細な説明は、文献を見ていただくのが良い。とりあえずここに実現プログラムを作るのに必要になる事を簡単に示す。

線形サーチ

検索というと真っ先に思い付くのがこの方法で、単純にデータを先頭から順番にアクセスし、探したいものを見つける。この方式のメリットはデータの順序がバラバラでかまわない点と、簡単にすぐに理解できて作ることが出来る点である。あとで出て来るバイナリサーチなどでは検索前にデータを整列しておく必要がある。デメリットは速度が遅い場合が多い点で、データの先頭の方に探したいものがあれば速いが、最悪の場合は全てのデータを見ることになってしまう。したがって、データ量が多ければ多い程速度の問題が大きくなって来る。なお、Ｃのライブラリに ｌｓｅａｒｃｈ（），ｌｆｉｎｄ（）という線形サーチの関数がある。

バイナリサーチ

プログラマーの間で最も人気のある方式で、先の線形サーチに比べ比較的簡単な準備だけで高速な検索を行なえる。ここでは使い方から見る。バイナリサーチは条件として、データが昇順にソートされている必要がある。これが実はこの方式のネックになるが、データが比較的固定的で、一度ソートしておいて、あとは検索を繰り返し行なうのみ、といった場合に良い。しかし、検索とデータの変更・追加が両方とも頻繁な場合には、データが変わるたびにソートしなくてはならない為、いくら検索が速くてもソートの時間がかかって総合的には全く速くない、という現象も起こり得る。この点には十分注意する必要がある。ソートは一般的に検索よりも時間がかかる。仕組みとしてはデータがソートされているので、適当に当たりをつけて（真中当たり）比較し、対象より大きければそれより手前の真中当たりで比較する、といった感じで探すので、全データを見る必要はない。はじめにデータをソートする。この時に使用する比較関数と検索で使う比較関数は同じ物を使わないと意味がない。ソートしたデータに対して、見つかればそのアドレスが返る。見つからない場合はＮＵＬＬが返る。見つかった時に配列のいくつめかを表示してる。一般的には構造体の配列などを探すのに使われ、構造体のメンバーで検索して、対象を得る場合には便利である。この検索方式は全データを見ずに結果が得られるので、先の線形検索に比べて高速である。ソートが問題なのですが、ソートにもいろいろなアルゴリズムがありますが、一般的にはここで使ったクイックソートが簡単で高速である。ただ、ソートも万能な物は無く、もとのデータのならびに特徴がある場合にはそれにあったアルゴリズムを使用すべきだ。クイックソートは比較的データの分散に依存せずに平均的に高速にソートする点が便利で良く使われる。

ハッシュサーチ

ハッシュサーチでは検索自体は圧倒的に高速である。仕組みとしてはデータをテーブルに格納する際に簡単な式でキーを割り当て、そのキーでダイレクトに飛べる場所にデータを格納しておく。検索の際は同様の式でキーを計算し、ダイレクトにその場所を得る。たとえば、文字列を格納したい場合にはその文字列のコードを全て足したものをキーとする。格納用のテーブルは普通は無制限には取れないので、全て足したものをテーブルの数で割った余りを実際のキーにする。キーが重複する可能性も十分あるので、それに対応する為、格納先を配列形式にしておいたり、そのキーから空いたテーブルを順に探したりする方法が取られている。テーブルに格納したい文字列を引数で渡し、格納先のキーが返る。そのキーを渡すと文字列が返る。文字列を渡し、それがテーブルに存在するかどうかを調べ、存在すればキーを返す。これらを使用すると、文字列を数値として管理が出来るようになり、長さ制限の無い文字列をプログラム中で整数として扱えるようになる。ある文字列に対して必ず唯一のキーが割り当てられるので、そのキーの値で比較なども行なえる。文字列の文字コードを全て足し、配列の大きさで割った余りと、その場所での配列の何番目かを併せて

キーにしている。一応、０はエラー判定に使う為に＋１した値を使っている。このようにハッシュサーチではキーを計算するだけで格納先に飛ぶので、データの個数がどれだけ増えても検索の時間は変わらない。逆検索および、登録の際ははじめのキーの計算先の配列の個数が増えて来ると徐々に時間がかかるようになるが、それでもはじめのキーの計算で分散性を良くしておけばあまり致命的に偏らないかぎりはそれほど速度が遅くなることはない。ハッシュサーチでは管理は面倒で、しかも、削除も出来ない、或いはしないほうが良いといった個性的な面もあるが、特に前記したような文字列のコード化などでは圧倒的な強さを見せる。登録した内容を変更しなくて良い場合には最適である。Cのライブラリにもｈｓｅａｒｃｈ（）という関数が用意されているが、１つしかテーブルを持てない点など不満もある。キーを計算するところでループを使っているが、そこのループの回数を減らしたりして高速化も可能だ。ここでは線形サーチ・バイナリサーチ・ハッシュサーチを取り上げたが、ツリー構造のデータを使った検索など、まだまだいろいろなアルゴリズムがある。万能な物はないので、高速な検索が必要となった場合は、データ構造から十分に検討し、最適な検索を用いる必要がある。いろいろな検索に対応する為に各種の検索専用テーブルを用意したりしたこともありますが、データを更新した際に検索用テーブルも併せて更新する手間や、テーブル自体のメモリー使用量を考えると、後付け方式はあまり効果が無い場合が多い。

【０１１】次ぎに具体的な攻撃について考えよう。まず、クラッカーによる第１の種類の攻撃として、一般にポートスキャン（Ｐｏｒｔ　Ｓｃａｎ）と言われる種類の攻撃がある。この攻撃は、ネットワークに直接的な損害を及ぼすものではないが、その前段階の攻撃として用いられることが多い。この攻撃では、クラッカーは、自身の管理下にあるホストから、攻撃対象のネットワークに対して、パケット内の宛先ＩＰアドレスや宛先ポート番号を適宜変更しながらＩＰパケットを繰り返し送信する。そして、それらのＩＰパケットに対する応答を上記ホストを介して観測する。これにより、攻撃対象のネットワークにおいて、ファイヤウォール等による制限を受けずに外部との通信に利用されているＩＰアドレスやポート番号を探索する。なお、ここで、前記ポート番号は、ＴＣＰあるいはＵＤＰ上で動作するアプリケーションソフトウェアのサービス種類（例えばｔｅｌｎｅｔ、ｆｔｐ、ｓｍｔｐ、ｔｆｔｐ等）を表すもので、ＩＰパケット内のＴＣＰヘッダあるいはＵＤＰヘッダに付与されるデータである。この種の攻撃では、上記のようなＩＰパケットの送信は、通常、専用的なツールソフトウェアを用いて行われ、攻撃対象のネットワークには、宛先ＩＰアドレスやポート番号が互いに異なり、且つ送信元ＩＰアドレスが同一であるようなＩＰパケットが比較的短時間内に多数、送信される。そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、少なくともその送信元ＩＰアドレスが互いに同一で且つ宛先ＩＰアドレス又は宛先ポート番号が互いに異なるものが所定数以上あるとき、第１の種類の前記攻撃がなされたことを検知する。これにより、ポートスキャンと言われる第１の種類の攻撃を確実に検知することができる。

次に、クラッカーによる第２の種類の攻撃として、一般にＳｙｎ－ｆｌｏｏｄと称される種類の攻撃がある。この攻撃は、ＴＣＰの特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、ＴＣＰでは二つのホスト間で通信を行う場合、まず、両ホスト間で論理的なコネクションの開設処理が行われる。このコネクション開設処理では、一方のホストから他方のホストに対してＳｙｎ用ＩＰパケットを送信する。ここで、該Ｓｙｎ用ＩＰパケットは、それを詳しく言えば、上記一方のホストのＩＰアドレスと他方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビットのうちのＳｙｎビットのみを「１」としたものである。そして、コネクション開設処理では、このＳｙｎ用ＩＰパケットを受けた他方のホストは、前記一方のホストに対してＳｙｎ／Ａｃｋ用ＩＰパケットを送信する。ここで、該Ｓｙｎ／Ａｃｋ用ＩＰパケットは、詳しくは、上記他方のホストのＩＰアドレスと一方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビットを共に「１」としたものである。さらに、コネクション開設処理では、このＳｙｎ／Ａｃｋ用ＩＰパケットを受けた前記一方のホストは、前記他方のホストに対してＡｃｋ用ＩＰパケットを送信し、このＡｃｋ用ＩＰパケットを前記他方のホストが受けることで、両ホスト間の論理的なコネクションの開設がなされる。なお、上記Ａｃｋ用ＩＰパケットは、詳しくは、前記Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビットのうちのＡｃｋビットのみを「１」としたものである。

【０１２】前記Ｓｙｎ－ｆｌｏｏｄは、このようなＴＣＰの特性を利用する攻撃である。この攻撃では、クラッカーは、攻撃対象のネットワークの特定のホストに対して、比較的短い時間内に多数のＳｙｎ用ＩＰパケットを送信する。そして、それらの各Ｓｙｎ用ＩＰパケットに対して上記特定ホストからＳｙｎ／Ａｃｋ用ＩＰパケットが送信されてきても、Ａｃｋ用ＩＰパケットをその特定ホストに送信しない。このような攻撃がなされたと

き、上記特定ホストは、最初に送信されてきたＳｙｎ用ＩＰパケットに対するＳｙｎ／Ａｃｋ用ＩＰパケットを送信した後、所定時間（一般に２分）は、その時間内にＡｃｋ用パケットが送信されてこない限り、そのＡｃｋ用パケットの受信待ち状態となる。そして、この状態で新たなＳｙｎ用パケットが送信されてくる毎に、上記特定ホストは、新たなＳｙｎ用パケットに応じたコネクション開設処理を順番に完結すべくその新たなＳｙｎ用パケットの情報を通信処理用のバッファ領域に蓄積していく。ところが、バッファ領域の大きさには限界があり、該バッファ領域が満杯になると、前記特定ホストは、ＴＣＰの通信処理やＴＣＰ上のサービス処理を行うことができなくなる。これにより、特定ホストがダウンすることとなる。この種の攻撃（Ｓｙｎ－ｆｌｏｏｄ）では、前述のように、比較的短い時間内に、比較的多くのＳｙｎ用ＩＰパケットが攻撃対象のネットワーク内の特定のホスト（特定のＩＰアドレスを有するホスト）に対して送信されてくる。また、これに応じて、当該特定のホストからネットワークの外部に向かって、比較的短い時間内に、多くのＳｙｎ／Ａｃｋ用ＩＰパケットが送信される。さらに、それらのＳｙｎ用ＩＰパケットあるいはＳｙｎ／Ａｃｋ用ＩＰパケットに対応して最終的に前記特定ホストに送信されてくるべきＡｃｋ用パケットがその特定ホストに送信されてこない。そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきたＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）に基づく複数のＳｙｎ用ＩＰパケットであって、少なくともその宛先ＩＰアドレスが互いに同一であるものが所定数以上あり、且つ、その各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有すると共に前記ＴＣＰに基づくＡｃｋ用ＩＰパケットが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知する。あるいは、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークからその外部に所定時間内に送信されたＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）に基づく複数のＳｙｎ／Ａｃｋ用ＩＰパケットであって、少なくともその送信元ＩＰアドレスがそれぞれ互いに同一であるものが所定数以上あり、且つ、前記ＴＣＰに基づくＡｃｋ用ＩＰパケットであって、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の宛先ＩＰアドレス及び送信元ＩＰアドレスを有するものが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知する。これにより、Ｓｙｎ－ｆｌｏｏｄといわれる第２の種類の攻撃を確実に検知することができる。次に、クラッカによる第３の種類の攻撃として、一般にＴｅａｒｄｒｏｐと称される種類の攻撃がある。この攻撃は、ＩＰパケットの分解（所謂ＩＰフラグメント）に係る処理の特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、ＩＰパケットは、インターネット上をルータを介して転送される過程で、各ルータのデータ処理容量の関係上、分解されることがある。また、各ルータにおいてＩＰパケットが転送される際にエラーが生じることもあり、このような場合には、ルータは、ＩＰパケットの再送信を行う。このため、ＩＰパケットの宛先ＩＰアドレスのホストでは、分解された一部の同じＩＰパケットが、複数受信されるということもある。このようなことから、ＩＰに基づく通信では、最終的にＩＰパケットを受け取るホスト（宛先ＩＰアドレスのホスト）は、受け取ったＩＰパケットが分解されたものであるとき、残りの全ての分解部分のＩＰパケットを受信するまで、各分割部分のＩＰパケットを蓄積保持する。そして、全ての分解部分のＩＰパケットを受信してから、それらを整理して元のＩＰパケットのデータを復元する処理を行う。前記Ｔｅａｒｄｒｏｐは、このようなＩＰパケットの分解に係る処理の特性を利用する攻撃である。この攻撃では、クラッカーは、比較的短い時間内に、多数の同じ分解部分のＩＰパケットを攻撃対象のネットワークの特定のホストに送信した上で、残りの分解部分のＩＰパケットをその特定ホストに送信する。このような攻撃がなされたとき、上記特定ホストは、最終的に残りの分解部分のＩＰパケットを受信したときに、そのＩＰパケットと、先に送信されてきた多量の分割部分のＩＰパケットとから元のＩＰパケットのデータを復元しようとする処理を行うため、その処理に長時間を要するものとなる。このため、該特定ホストは、事実上、ダウンしてしまうこととなる。この種の攻撃（Ｔｅａｒｄｒｏｐ）では、前述の如く、比較的短い時間内に、多数の同じ分解部分のＩＰパケットがネットワーク内の特定のホストに送信されてくる。そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の分割されたＩＰパケットであって、同一の分割部分が所定数以上あるとき、第３の種類の前記攻撃がなされていることを検知する。これにより、Ｔｅａｒｄｒｏｐといわれる第３の種類の攻撃を確実に検知することができる。次に、クラッカーによる第４の種類の攻撃として、一般にＬａｎｄと称される種類の攻撃がある。この攻撃は、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるような、正規にはあり得ないＩＰパケットを、攻撃対象のネットワークの特定のホストに送信する攻撃である。このようなＩＰパケットを送信された特定ホストは、そのＩＰパケットの処理に手間取ることが多く、ダウンしてしまうことがしばしばある。

【０１３】この種の攻撃では、上記の如く、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるＩＰパケッ

トが、ネットワーク内の特定のホストに送信される。しかも、一般には、そのようなＩＰパケットが比較的短い時間内に、複数、上記特定ホストに送信される。そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、その送信元ＩＰアドレスが宛先ＩＰアドレスと同一のアドレスとなっているものが所定数以上あるとき、第４の種類の前記攻撃がなされていることを検知する。これにより、Ｌａｎｄとわれる第４の種類の攻撃を確実に検知することができる。なお、前述したＳｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄといわれる攻撃は、一般に、ＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）といわれる種類の攻撃に属するものである。そして、このＤｏＳには、Ｓｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄのほかに、例えばＳｍｕｒｆといわれる種類の攻撃や、Ｆｌｏｏｄｉｅといわれる種類の攻撃等もある。本明細書では、ＤｏＳに属する種類の攻撃として、代表的にＳｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄを挙げたが、ＳｍｕｒｆやＦｌｏｏｄｉｅ等の攻撃を検知するようにすることも可能である。前述のようにクラッカーによる攻撃を検知する攻撃検知手段を備えた本発明では、前記処理手段が行う処理は、例えば前記攻撃が検知された旨を表す報知出力を発生する処理である。この報知出力の発生により、ネットワーク管理者やあるいは外部の専門技術者等が、検知された攻撃を排除するための処置を施すことが可能となる。あるいは、前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、前記攻撃を検知してから所定時間阻止する処理である。

【０１４】高速検索アルゴリズムとしては、タイムキュー付きのハッシュ法を利用している。その具体的な特徴は以下の実施例にしめした。一方、コーディング方式としては、ＬＩＮＵＸのｋｅｒｎｅｌ－ｃｏｄｉｎｇを採用した。従って、ＯＳの機能を利用せず、直接インターフェースとやりとりをするプログラムを作製した。これは開発にかなりの時間を要する事になったが、できたソフトの速度は大変高いものとなった。一般に、インターフェースとのやりとりはＯＳの主要な仕事であり、ＯＳの利用者はそれをインターフェースの付いたサブルーチンとして提供を受ける事ができる。そうすれば、通常のＵＮＩＸ（登録商標）ユーザーには公開されていない、例えばメモリー管理情報にもアクセスする必要がなくなるのだが、ここでは、速度を重視したため、直接駆動するコードを作製した。ＯＳはいろいろなハードウェア環境全体を効率よく管理する目的の為には、有望だが、単一の機能に特化してパフォーマンスを上げるためには、避ける必要が出ていた。従来の類似の技術では、ここまでの開発は行わないため、比較的短時間で開発が済む代わり、性能的には低速になっていた。今回、世界で始めて開発された部分である。単なる検出だけなら、ここまでの高速性は不要である、というのは、機械から見ると遅くとも、人間にとって充分早い程度の時間（例えば１～２秒）の内に、記録を残せば充分であったからである。今回、我々は、パケットが通過するまでの時間（１／１０００秒程度）に、判断して遮断する必要があったため、高速のアルゴリズムおよび、高速のプログラム実行方式を用意せざるを得なかったのである。そして、高速で処理の実をフルに生かした製品が出来上がっている。他にも、ハッシュ値の表が時間とともに変化する機能が存在している。古いパケットの情報は自動的に消滅するのである。インターネットの攻撃、それも特にＤｏＳと言われる攻撃に対抗するには、一定の時間内にある程度の数の攻撃パケットに対応できる能力が必要になる。これの作り込みに、タイムキューの果たす役割は重要になっている。また、各パケットの間が、あまりに長時間の場合はＤｏＳとしての攻撃の効果は薄れるため、消去の設定が必要となる。

【０１５】

【発明の実施の形態】　本発明の一実施形態を図１を参照して説明する。図１は本実施形態のシステム構成図である。図１において、１はネットワークとしてのＬＡＮである。このＬＡＮ１は、例えばイーサネット（登録商標）（Ｅｔｈｅｒｎｅｔ（登録商標））を用いて構築されたものであり、図示を省略する複数のホスト（コンピュータ）がイーサネット・ケーブルやハブ等を介して接続されている。各ホストには、それをイーサネット・ケーブルに接続するイーサネット・カードや、ＴＣＰ／ＩＰの処理を行うためのソフトウェア、ＴＣＰ／ＩＰ上で機能する各種アプリケーションソフトウェア（例えば、ｔｅｌｎｅｔ、ｆｔｐ、ｓｍｔｐ等）が実装され、ＩＰに基づく通信を可能としている。なお、ＬＡＮ１は、イーサネット上で構築されたものに限らず、トークンリング等、他の形態で構築されたものであってもよい。本実施形態のシステムでは、ＬＡＮ１の入り口に、パケットフィルタとしてのファイヤウォールの機能をもたせたコンピュータ２（以下、このコンピュータ２を単にファイヤウォール２と称する）が設けられている。そして、ＬＡＮ１はファイヤウォール２を介してインターネット３に接続されている。ファイヤウォール２は、どのような種類のＩＰパケットのＬＡＮ１への進入を禁止するかを規定するデータが書き込まれるファイル（以下、フィルタ設定ファイルという）を有している。そして、ファイヤウォール２は、このフィルタ設定ファイルで、ＬＡＮ１への進入が禁止された種類のＩＰパケットがインターネット３側から送信されてきたときに、そのＩＰパケットを廃棄してＬＡＮ１への進入を阻止する。また、フィルタ設定ファイルで、ＬＡＮ１への進入が禁止されてい

ないＩＰパケットが送信されてきたときには、それをＬＡＮ１に転送する。ファイヤウォール２とインターネット３との間には、ハブ４が介装され、このハブ４に攻撃検知手段の機能をもたせたセンサ５が接続されている。また、このセンサ５には、前記ファイヤウォール２を制御する処理手段の機能を有するディレクタ６が接続されている。これらのセンサ５及びディレクタ６はそれぞれコンピュータにより構成されたものである。前記センサ５は例えばＵＮＩＸマシンにより構成され、イーサネットカード７を介して前記ハブ４に接続されている。この場合、センサ５には、ｔｃｐｄｕｍｐといわれるソフトウェアが実装されている。このｔｃｐｄｕｍｐによって、ハブ４を通る全てのＩＰパケットをイーサネットカード７を介して取得する（ヒアリングする）ことができる。このような動作は、プロミス・キャス・モード（ｐｒｏｍｉｓｅ　ｃａｓｔ　ｍｏｄｅ）といわれることが多い。そして、センサ５は、取得した各ＩＰパケットをその取得時点の時刻データと共に図示しないハードディスクに記憶保持するようにしている。なお、ハードディスクに記憶保持したＩＰパケットの総量が所定の許容量に達したときには、センサ５は、最も古いＩＰパケットを消去し、新たに取得されたＩＰパケットをハードディスクに記憶保持する。また、センサ５は、ＩＰアドレスを持たず、ＡＲＰ（Ａｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）や、ＲＡＲＰ（Ｒｅｖｅｒｓｅ　Ａｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）のパケット等、応答を促すパケットが送信されてきても、それに対する応答をしないようにソフトウェア的に設定されている。つまり、センサ５はＩＰパケットの受信（取り込み）のみを行うことできるものとされている。さらに、センサ５には、前述した第１～第６の種類の攻撃を検知するためのソフトウェア（以下、攻撃検知アルゴリズム）が実装されている。なお、この攻撃検知アルゴリズムは、ディレクタ６に実装しておき、該ディレクタ６とのデータ授受を行いつつ該攻撃検知アルゴリズムの処理をセンサ５に行わせるようにしてもよい。前記ディレクタ６には、前記ファイヤウォール２を制御するソフトウェア（以下、フィルタ制御アルゴリズムという）が実装されている。この場合、フィルタ制御アルゴリズムは、センサ５により検知される攻撃に応じて、前記フィルタ設定ファイルのデータを適宜書き換えることで、前記ファイヤウォール２を制御するものである。

【０１６】次に、かかる本実施形態の作動を説明する。前記センサ５は、取得されるＩＰパケットを前述の如くハードディスクに記憶保持しつつ、所定のサイクルタイム毎に次のような処理を行う。すなわち、センサ５は、ハードディスクから所定の時間間隔分の複数のＩＰパケットを、送信元ＩＰアドレス及び宛先ＩＰアドレスの値別に分類した上で、図示しないメモリに取り込んで保持する。つまり、所定の時間間隔分の複数のＩＰパケットのうち、同一の送信元ＩＰアドレスを有するものをひとまとめにすると共に、同一の宛先ＩＰアドレスを有すものをひとまとめにして、メモリに取り込む（以下の説明では、このようにひとまとめにされたＩＰパケットの組をＩＰパケット群という）。そして、このメモリに取り込んだ複数のＩＰパケットに対して、後述する攻撃検知の処理を行った上で、それらのＩＰパケットをメモリから消去する。この場合、各サイクルタイムにおいて、メモリに取り込むＩＰパケットは、前回のサイクルタイムでメモリに取り込んだＩＰパケットのうちの最も古いＩＰパケットの取得時刻から所定時間を経過した時刻以後に取得されたものである。各サイクルタイムにおけるセンサ５による攻撃検知の処理は、攻撃検知アルゴリズムに従って次のように行われる。センサ５は、まず、前記第１～第６の種類の攻撃のうち、例えば、第１の種類の攻撃、すなわちポートスキャンを検知する処理を行う。この処理では、センサ５は、メモリに前述のように取り込んだＩＰパケットのうち、送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１の外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ＩＰアドレスの値（これはＬＡＮ１に属するＩＰアドレスの値である）を抽出する。そして、上記の各ＩＰパケット群で抽出した宛先ＩＰアドレスの各値に対し、そのＩＰパケット群（同一の送信元ＩＰアドレスのＩＰパケット群）から、該宛先ＩＰアドレスの値と同一の宛先ＩＰアドレスを有し、且つＴＣＰヘッダあるいはＵＤＰヘッダ内の宛先ポート番号が互いに異なり、且つ、連続した所定時間内（例えば３０秒内）に取得されたＩＰパケットの個数をカウントする。このとき、このカウント数が所定数（例えば２０個）に達した場合には、センサ５は、ポートスキャンの攻撃がなされていることを検知する。そして、そのことを示すデータと、この攻撃が検知されたＩＰパケット群の送信元ＩＰアドレスの値データとを（以下、これらのデータを第１種攻撃検知データという）前記ディレクタ６に与える。このような処理が送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１に属さない全てのＩＰパケット群に対し順次行われる。なお、本実施形態におけるポートスキャンの検知では、ポート番号が互いに異なるＩＰパケットの個数をカウントするようにしたが、次のような処理によりポートスキャンを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で、且つ、該送信元ＩＰアドレスがＬＡＮ１外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ポート番号の値を抽出する。さらに、その抽出した宛先ポート番号の各値に対し、該宛先ポート番号を抽出したＩＰパケット群から、該宛先ポート番号の値と同一の宛先ポート番号を有し、且つ宛先ＩＰアドレスが互いに異なり、且つ、連続した所定時間内に取得され

たＩＰパケットの個数をカウントする。そして、そのカウント数が所定数に達した場合にポートスキャンが行われていることを検知する。一方、センサ５から前述のような第１種攻撃検知データを与えられた前記ディレクタ６は、該第１種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば５分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ポートスキャンの攻撃からＬＡＮ１が保護される。なお、ディレクタ６は、上記所定時間（５分間）が経過するまでの間に、先に与えられた第１種攻撃検知データと同一の第１種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（５分間）、該第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、ポートスキャンの攻撃が続いている限り、その送信元ＩＰアドレスからのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（５分間）が経過するまでに、前記第１種攻撃検知データが与えられなかった場合には、その第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のようにポートスキャンの攻撃の検知処理を行ったセンサ５は、次に、第２の種類の攻撃（Ｓｙｎ－ｆｌｏｏｄ）の検知処理を行う。

【０１７】この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳｙｎ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各Ｓｙｎ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳｙｎ用ＩＰパケットが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否か調べる。そして、そのようなＳｙｎ用ＩＰパケットが存在する場合には、先に抽出したＳｙｎ用ＩＰパケットを含めてそれらのＳｙｎ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳｙｎ用ＩＰパケットに対して、それぞれに対応するＡｃｋ用ＩＰパケット（詳しくは該Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレスを有し、且つ、該Ｓｙｎ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のシーケンス番号を有するＡｃｋ用ＩＰパケット）であって、且つ該Ｓｙｎ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否かを調べる。このとき、そのようなＡｃｋ用ＩＰパケットが存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡｃｋ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、Ｓｙｎ－ｆｌｏｏｄの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＳｙｎ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第２種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。なお、本実施形態では、Ｓｙｎ用ＩＰパケットの個数に基づいてＳｙｎ－ｆｌｏｏｄを検知したが、次のような処理によりＳｙｎ－ｆｌｏｏｄを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で且つ、該送信元ＩＰアドレスがＬＡＮ１に属する各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳｙｎ／Ａｃｋ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各Ｓｙｎ／Ａｃｋ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳｙｎ／Ａｃｋ用ＩＰパケットが、同じ送信元ＩＰアドレスのＩＰパケット群内に存在するか否か調べる。このとき、そのようなＳｙｎ／Ａｃｋ用ＩＰパケットが存在する場合には、先に抽出したＳｙｎ／Ａｃｋ用ＩＰパケットを含めてそれらのＳｙｎ／Ａｃｋ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳｙｎ／Ａｃｋ用ＩＰパケットに対して、該Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスのＩＰパケット群を調べる。このとき、該Ｓｙｎ／Ａｃｋ用ＩＰパケットに対応するＡｃｋ用ＩＰパケット（詳しくは該Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有し、且つ、該Ｓｙｎ／Ａｃｋ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のＡｃｋ番号を有するＡｃｋ用ＩＰパケット）であって、且つ該Ｓｙｎ／Ａｃｋ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、当該ＩＰパケット群内に存在するか否かを調べる。そして、そのようなＡｃｋ用パケットが存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡｃｋ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、Ｓｙｎ－ｆｌｏｏｄの攻撃がなされていることを検知する。

【０１８】なお、この場合にセンサ５からディレクタ６に与えるデータは、Ｓｙｎ－ｆｌｏｏｄの攻撃を検知したことを示すデータと、上記Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データである。この場合、Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先Ｉ

ＰアドレスのＩＰアドレスの値データは、それぞれ、先に説明した前記第２種攻撃検知データにおけるＳｙｎ用ＩＰパケット宛先ＩＰアドレスの値データ、送信元ＩＰアドレスの値データに相当するものである。一方、センサ５から前述のような第２種攻撃検知データを与えられた前記ディレクタ６は、該第２種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、ディレクタ６は、第２種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケット、あるいは上記宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、Ｓｙｎ－ｆｌｏｏｄの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（２分間）が経過するまでの間に、先に与えられた第２種攻撃検知データと同一の第２種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（２分間）、該第２種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。このことは、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除についても同様である。従って、Ｓｙｎ－ｆｌｏｏｄの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレスからのＩＰパケット、あるいはその攻撃に係る宛先ＩＰアドレスへのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除と、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除とのいずれについても、それぞれに対応する上記所定時間（２分間、２秒間）が経過するまでに、前記第２種攻撃検知データが与えられなかった場合には、その第２種攻撃検知データの送信元ＩＰアドレスを有するＩＰパケット、あるいは、第２種攻撃検知データの宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のようにＳｙｎ－ｆｌｏｏｄの攻撃の検知処理を行ったセンサ５は、次に、第３の種類の攻撃（Ｔｅａｒｄｒｏｐ）の検知処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれる分轄されたＩＰパケット（以下、単に、分轄パケットという）を順次抽出する。この場合、ＩＰでは、分轄パケットは、そのＩＰヘッダ中の特定のフラグが「１」となっているか、もしくは、フラグメントオフセットといわれるデータが「０」より大きな値となっている。これにより、分轄パケットを見出すことができる。そして、センサ５は、抽出した各分轄パケットの取得時刻から所定時間（例えば５分間）内に取得され、且つ、該分轄パケットとＩＰヘッダ中のＩＰ識別番号及びフラグメントオフセットの値がそれぞれ同一であるもの（抽出した分轄パケットと同一の分轄パケット）が、該分轄パケットと同じＩＰパケット群内にあるかを調べる。このとき、そのような分轄パケットがある場合には、先に抽出した分轄パケットを含めてそれらの分轄パケットの個数をカウントする。そして、このカウント数が所定数（例えば８０個）以上である場合には、Ｔｅａｒｄｒｏｐの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された分轄パケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第３種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第３種攻撃検知データを与えられた前記ディレクタ６は、前記Ｓｙｎ－ｆｌｏｏｄが検知された場合と全く同じやり方で、ファイヤーウォール制御する。すなわち、第３種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、第３種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。これにより、Ｔｅａｒｄｒｏｐの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。

【０１９】上記のようにＴｅａｒｄｒｏｐの攻撃の検知処理を行ったセンサ５は、次に、第４の種類の攻撃（Ｌａｎｄ）の検知処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群から、該ＩＰパケット群の宛先ＩＰアドレスと同じ値の送信元ＩＰアドレスを有するＩＰパケットを抽出する。さらに、その抽出したＩＰパケットと同じ宛先ＩＰアドレスのＩＰパケット群の中から、該ＩＰパケットと

同じ送信元ＩＰアドレスを有し、且つ該ＩＰパケットの取得時刻から所定時間（例えば２分間）内に取得されたＩＰパケットが存在するか否かを調べる。そして、そのようなＩＰパケットが存在する場合には、先に抽出したＩＰパケットを含めてそれらのＩＰパケットの該ＩＰパケットの個数をカウントする。このとき、該カウント数が所定数（例えば６個）以上である場合には、Ｌａｎｄの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データを（以下、これらのデータを第４種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第４種攻撃検知データを与えられた前記ディレクタ６は、第４種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有し、且つ、該送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば３分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、Ｌａｎｄの攻撃からＬＡＮ１が保護される。この場合、ポートスキャンの検知時の場合と同様、ディレクタ６は、第４種攻撃検知データにおける送信元ＩＰアドレスと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（６分間）が経過するまでの間に、先に与えられた第４種攻撃検知データと同一の第４種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（６分間）、該第４種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、Ｌａｎｄの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（６分間）が経過するまでに、前記第４種攻撃検知データが与えられなかった場合には、その第４種攻撃検知データの送信元ＩＰアドレスと同一の送信元ＩＰアドレス及び宛先ＩＰアドレス有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。なお、本実施形態では、第４種攻撃検知データとして、Ｌａｎｄの攻撃に係るＩＰパケットの送信元ＩＰアドレスの値データをディレクタ６に与えるようにしたが、Ｌａｎｄの攻撃に係るＩＰパケットの送信元ＩＰアドレスと、宛先ＩＰアドレスとは同じ値である。従って、その送信元ＩＰアドレスの値データの代わりに、宛先ＩＰアドレスの値をディレクタ６に与えてもよいことはもちろんである。前述のように、Ｌａｎｄの攻撃の検知処理を行ったセンサ５は、次に第５の種類の攻撃（パスワードの獲得）を検知する処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、ＬＡＮ１のホストのユーザ名データ及びパスワードデータを含むＩＰパケットを抽出する。それらの抽出したＩＰパケットの中から、ユーザ名データが同一で、且つ、パスワードデータが互いに異なり、且つ、連続した所定時間（例えば２分間）内に取得されたＩＰパケットの個数をカウントする。このとき、このカウント数が所定数（例えば２０個）以上であれば、クラッカーがパスワードを獲得するための第５の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第５種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第５種攻撃検知データを与えられた前記ディレクタ６は、該第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば１時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、パスワードの獲得を狙った第５の種類の攻撃からＬＡＮ１が保護される。

【０２０】なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第５種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（１時間）が経過するまでの間に、先に与えられた第５種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（１時間）、該第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、第５の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（１時間）が経過するまでに、前記第５種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス

及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のように、第５の種類の攻撃の検知処理を行ったセンサ５は、次に第６の種類の攻撃（セキュリティホールの攻撃）を検知する処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、例えばプリンタの論理名である「Ｉｐｒ」を有し、且つ、データサイズが１２８文字以上であるＩＰパケットを検索する。そして、そのようなＩＰパケットが見つかった場合には、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第６種攻撃検知データという）前記ディレクタ６に与える。一方、センサ５から前述のような第６種攻撃検知データを与えられた前記ディレクタ６は、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば４時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃からＬＡＮ１が保護される。なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第６種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（４時間）が経過するまでの間に、先に与えられた第６種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（４時間）、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、第６の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（４時間）が経過するまでに、前記第６種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットＩＰパケットのＬＡＮ１への進入の阻止を解除する。以上説明したようにして、本実施形態のシステムによれば、センサ５や、ディレクタ６を導入するだけで、クラッカーによるＬＡＮ１への各種の攻撃をリアルタイムで検知しつつ、検知された攻撃からＬＡＮ１を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮してＬＡＮ１を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、ひいては、ＬＡＮ１の維持管理のコストを低減することができる。また、クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、ＬＡＮ１と外部との通信を格別に制限する必要性が少なくなる。このため、通常時は、ＬＡＮ１の通信の自由度を高めることができ、インターネット３上の情報資源を有用に活用することができる。なお、以上説明した実施形態では、ＬＡＮ１の入り口にファイヤウォール３を設けておき、クラッカーによる攻撃が検知されてとき、該ファイヤウォール３を制御することで、検知された攻撃を自動的に排除する処置を行った。但し、クラッカーによる攻撃が検知されたときに、単に、その旨の報知をネットワーク管理者や、専門の警備管理者等に行うようにしてもよい。この場合には、例えば前記ディレクタ６あるいはセンサ５を公衆回線や専用回線を介してネットワーク管理者や、警備管理者等のホストに接続しておく。そして、攻撃が検知された場合に、前述した第１乃至第６種攻撃検知データのような情報をネットワーク管理者や警備管理者等のホストにディレクタ６あるいはセンサ５から送信する。このようにしたときには、検知された攻撃からＬＡＮ１を保護するための具体的な処置は、ネットワーク管理者等が直接的に行うこととなる。しかるに、この場合であっても、ネットワーク管理者等は、上記の報知を受けたときに処置を施せばよく、しかも攻撃の種類は検知されるので、攻撃に対する処置を比較的容易に施すことができる。また、前記実施形態では、第１乃至第６の種類の攻撃を順番に検知するものを示したが、それらの攻撃の検知処理を並列的に行うようにすることも可能である。また、前記実施形態では、前述したＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）に属する攻撃のうち、Ｓｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄを検知するものを示した。但し、この他にも、ＤＤｏＳ（ｄｉｓｔｒｉｂｕｔｅｄ　Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）ＳｍｕｒｆやＦｌｏｏｄｉｅといわれるような攻撃を検知するようにすることも可能である。

【０２１】産業上の利用可能性

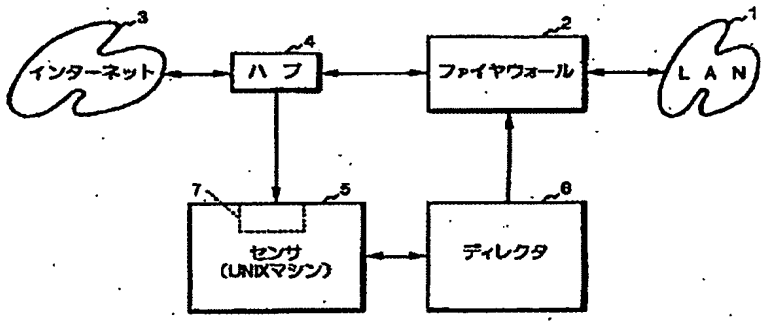
以上のように、本発明のクラッカー監視システムは、企業や官庁等の組織に構築されたＬＡＮ等のネットワークをクラッカーによる攻撃から簡易に保護し、また、その保護を通信の自由度を必要以上に損なうことなく行うことができるシステムとして有用である。

【図面の簡単な説明】

【図１】　図１は、本発明のクラッカー監視システムの一実施形態のシステム構成図である。

【図１】

FIG. 1



# PU020277 (JP2002124996) ON 8340

(19) Patent Agency of Japan (JP)
(12) Official report on patent publication (A)
(11) Publication number: 2002-124996
(43) Date of publication of application: 26.04.2002
(51) Int.Cl. H04L 12/66 G06F 13/00
(21) Application number: 2000-350265
(22) Date of filing: 13.10.2000
(71) Applicant: Baba Yoshimi
(72) Inventor: Baba Yoshimi
(54) Title of the invention: Fast packet acquiring engine/security

(57) Abstract:

Problem to be solved: To provide a cracker monitor system of a simple system configuration to protect an LAN 1 from attacking by a cracker by automatically detecting the attack by the cracker to the LAN 1 with no burdensome limit on communication or experienced engineers.

Solution: A sensor 5 is provided where a hash algorithm is used to sequentially acquire IP packets passing an entrance of a LAN 1. The sensor 5 quickly detects various attacks by a cracker to the LAN 1 based on the acquired IP packet. The information related to the attack which is detected by the sensor 5 is provided to a director 6 controlling a fire wall 2.

The director 6 controls setting of the fire wall 2 according to the supplied information and prevents an IP packet related to the detected attack from entering the LAN 1.

## [Claims]

[Claim 1] A device for communication that carries out the detecting elements of it to within a time that passes the packet without delay and includes the feature in apparatus that passes a packet that flows through a network at high speed for suitable processing to be performed.

[Claim 2] The device for communication according to claim 1 that compress transmission and receipt information by a hash method, and have the feature to have made it possible to develop all information in sufficiently narrow memory space.

[Claim 3] The device for communication according to claim 1 or 2 that includes the feature to achieve a well head by using double hash and a list mode at the time of hash table production.

[Claim 4] The device for communication according to claim 1 or 2 or 3 that controls a compression ratio to hash table utilization time and includes the feature by maintaining a memory capacity factor to about 80% to achieve a well head avoiding a collision.

[Claim 5] The device for communication according to claim 1 or 2 or 3 or 4 aiming at intercepting and detecting of an attack called hacking or cracking on

the Internet, especially TCP-Syn Flood, Teadrop, Land, Pingof Death, and Distributed Denial of Service.

[Claim 6] The device for communication according to claim 1 or 2 or 3 or 4 or 5 that has the feature to supplement with communication data about it at high speed when an attack of wresting a password of a route takes place, buffer overflow of a bug of OS, and the like is made to cause using communication on the Internet.

## [Detailed description of the invention]

[001]

[Field of the invention] This invention supervises the attack to the network (LAN) through the Internet by a cracker, and relates to the system for protecting a network from the attack further.

[Description of the prior art] In recent years, the majority is connected to the Internet and, as for the network (LAN) built by in-houses, such as a company, the exchange (communication) of the variety of information between other networks is performed via the Internet. In this communication, generally, IP (Internet Protocol) is used as a protocol mainly corresponding to the network layer what is called in an OSI layer model, and communication data is exchanged with the embodiment of an IP packet.

And as a protocol (protocol of the higher rank of IP) mainly corresponding to the transport layer of the higher rank of the mentioned above network layer, usually uses TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).

[002]

This kind of network has the advantage that various information can be exchanged by low cost between the server on the Internet, other networks and the like. Since the Internet has very advanced glasnost on the other hand, it will be exposed to the danger of receiving the attack from what is called a cracker. For this reason, it is required that a network should be protected from such an attack. The system that provided conventionally the fire wall (computer that has the function of the fire wall in details) as a system for protecting such a network in the entrance of the network which it is going to protect is known. This fire wall prevents that communication of the kind which the network administrator etc. defined preliminary is performed between that exterior in a network, and enables it to perform only the permitted other communication between that exterior in a network. In this case, specification of the kind of communication to prevent is enabled by a transmitting agency IP address, destination IP addresses, a destination port number, and so on that are included, for example in an IP packet. The host that has a specific IP address in a network according to such a fire wall (computer) or access from the outside to the

host's specific port number can be forbidden or access to the network from IP addresses other than the specific IP address of the network exterior can be forbidden. Thus, if the kind of communication data that forbids the penetration to a network is appropriately set up to the fire wall, it is possible to reduce the danger of the attack to a network.

[003]

As a system for detecting the attack to such a network, the system that provided conventionally the intrusion detection system (computer that has in English intrusion detection system and the function to detect an invader's communication pattern in detail) in the entrance of the network that it is going to protect is known. This intrusion detection system detects that communication of a pattern peculiar to the aggressor of the kind collected preliminary is performed between that exterior in a network, and notifies it to an administrator. Here, since the detection takes time, such as collection of data, and reference of a database, it is usually impossible to intercept it based on detection of an attack hav ing been delivered or to enable it to perform only the permitted other communication between the exterior in a network. In this case, in order to prevent communication, considerably until an IP packet passes, for example between short time, since detection specification must be enabled by the information that are included in communication, in the sniffer that is a tool for the usual packet check or BPF (Bakley Packet Filter), it is

too late. Thus, being the exterior of the inside of a network and a network also by an intrusion detection system, and forbidding invasion to a network also by a fire wall, cannot be lost, even if it sets up appropriately and can reduce the danger of the attack to a network. That is, in order to defend by the fire wall or an intrusion detection system, each host in the network that it is going to protect uses what kind of information or it had to determine synthetically whether it should provide outside and information like the throat in a network should be protected or what kind of thing was assumed as an attack expected and there was an impossible situation also by a remarkable skilled technique person depending on the case.

[004]

Thus, network management had always taken the great labor and cost by a skilled technique person accompanied by restoration on condition of being attacked. The above conventional fire walls tend to eliminate all communications with an offensive possibility. Thus, communication of the kind forbidden by setting out is uniformly eliminated irrespective of whether it is what the communication depends on the attack from a cracker. That is, the flexibility of communication with a network and the exterior is restricted more than needed. For this reason, in the network provided with the fire wall, restriction of the available informational service on the Internet is received.

As a result, the inconvenience that many information resources on the Internet are unenjoyable useful is produced.

[005]

[Problems to be solved by the invention] This invention is made in view of this background, the purpose detects automatically the attack from the cracker that it is alike and is received, restricts communication more than needed. It is providing the cracker monitoring attack interception system that can aim at protection of the network to the attack from a cracker by a simple system configuration, without needing the labor by a skilled technique person.

[Means for solving the problem] This invention is characterized by a cracker monitor system in order to attain this purpose including acquiring an IP packet that passes through this entrance at an entrance of a network which performs communication based on IP (Internet Protocol) one by one, and it is held cumulatively, an attack detection means to detect an attack from a cracker to this network by supervising a plurality of held IP packets, a processing means to perform predetermined processing according to it when this attack detection means detects the mentioned above attack.

[006]

That is, when an invention in this application person examines the technique of various attacks by a cracker, generally many kinds of attacks have mutual

relevance characteristic of a plurality of IP packets that communicate serially in the case of the attack, respectively. Thus, an IP packet that passes through that can be acquired one by one by the mentioned above attack detection means and can be held cumulatively at an entrance of the mentioned above network, and an attack to the mentioned above network by a cracker can be detected in real time by supervising a plurality of the held IP packets. And if an attack is detectable in this way, protection of a network from the attack can be aimed at by performing suitable processings (for example, information to a network administrator and the like, processing that intercepts communication by a cracker, and so on) by the mentioned above processing means according to it. In this case, in order for sufficient accuracy to improve an attack by a cracker detection defense, generally in short, remarkable high speed is gone on. For this reason, in order to detect an attack, an algorithm of a hash table is required as a technique that accumulates information about an IP packet at high speed. Or if treatment for protecting a network by it is performed, network damage can fully be suppressed.

[007]

What is necessary is to take measures against an attack only then, when the detection is made since an attack by a cracker is detectable in real time according to the system of such this invention.

For this reason, the necessity that network administrators refer to frequently what is called a log file (communication recording book) is reduced. A labor that takes an attack by a cracker into consideration in prediction in the cases, such as network construction and reorganization, is lightened. There is no necessity for which an attack is not detected of predicting an offensive possibility and restricting communication with a network and its exterior, at the time, and it can usually raise flexibility of the communication. Thus, according to this invention, an attack from a cracker to a network is detected automatically, and protection of a network to an attack from a cracker can be aimed at by a simple system configuration, without restricting communication more than needed or needing a labor by a skilled technique person. In this invention, the mentioned above attack detection means constitutes all IP packets that pass through an entrance of the mentioned above network in ability ready for receiving. This becomes possible to detect many kinds by a cracker of attacks promptly. Only reception of an IP packet constitutes the mentioned above attack detection means from this invention possible.

[008]

According to this, the existence is not recognized by a cracker and the like or the mentioned above attack detection means is not made into an offensive object, in order not to transmit data of self-information, such as self IP address, MAC (Media Access Control)

address, and the like to a network. Thus, the safety of an attack d etection means can be secured and the reliability of a system of this invention can be secured by extension. In this invention, the mentioned above attack detection means detects an attack of several kinds based on the mentioned above algorithm from the mentioned above a plurality of IP packets that held an algorithm for detecting an attack of several kinds to the mentioned above attack of a plurality of kinds, and were acquired and held. This is enabled to detect an attack of a plurality of kinds depended on a cracker, and the safety of the mentioned above network can be improved. It becomes possible to correspond also to a new kind of attack by updating the mentioned above algorithm suitably. In this case, a plurality of IP packets that acquired the mentio ned above attack detection means and were held as a means to classify according to a transmitting agency IP address and/or destination IP addresses at least, a solid casting type list hash method is provided and an attack of the mentioned above several kinds is detected from a table for a plurality of the classified IP packets.

[009]

That is, in order to detect an attack of a plurality of kinds, a transmitting agency IP address and destination IP addresses (these are given to an IP header of an IP packet) of an IP packet serve as an important key in many cases. Thus, it becomes easy to detect an attack by classifying an IP packet acquired in predetermined time according to a transmitting

agency IP address and/or destination IP addresses and holding it from those IP packets. More specifically in this invention, the mentioned above attack detection means detects an attack by a hash table as follows. A hash method (hashing) is a technique for searching data at high speed on a memory. Unlike various kinds of 3 structures, it can mount easily only in static arrangement, and efficiency is very high too. There are some techniques of searching data on arrangement. Next, it explains sequentially from a simple technique and results in explanation of a hash method. I will consider a case where certain information is processed on a memory. It only decides that a number (integer) is used as a key of information, and it is carried out to not considering others.

(1) Simple array data

Stuffing an appearance order of arrangement, but a simple and fundamental method, although insertion of data is high-speed, since search must be seen sequentially from an end (it is called linear search), when it averages, processing is needed about a half of the data number. Since this technique is late, when there are many data numbers, it is as good as ... that is not used, but although many programmers learn only this method thus, it is used also when there is much number of cases actually.

(2) Sorted arrangement

Aligning data on arrangement in order of a key (in this case, staff number), if it carries out like this insertion of data time starting (mentioned below), since a technique of binary search can be used for search at most, it ends by processing of a log (N) time. Since it is data of 1 million contacts or log(N) =20, a vast quantity of data is very high speeds too. On the other hand, cost (processing time) starts maintenance of data, a case where the contents of data are fixed (example: keyword of Visual Basic ... print and the like), since data can be collectively sorted when a phase when it is generated by data, and a phase referred to are divided clearly (a line type of DXF, and a complex graphic definition), if high-speed algorithms, such as quick sort, are used, it will be the time and effort of N*log (N). This does not have various kinds of tree structures and inferiority.

However, when using it, collecting data, data must be inserted in sorted arrangement, and processing time requires an order of a square of N, that is, is late.

(3) Reverse length table

It is a premise of small data, it will consider a case where a number is an integer of triple figures, as a special case. In this case, a number has only 1000 kind weakness of 001-999. For this reason, arrangement of 1000 elements is prepared preliminary and there is a method of putting into arrangement by making a number into an index.

This is called reverse length table, a pseudo code in a case of putting in information is as follows.

**master [number] = contents**

Registration and search are high speeds very much, and an advantage of reverse length table is that processing is also simple. On the other hand, a problem is being unable to use, unless the range of a key is small. For example, by large data, since a number is 9 or more figures, it has 1 billion kinds of possibilities, and a reverse length table is not realistic. For this reason, a reverse length table is not so common.

(4) Hash table

A number of large data as mentioned above comes out of 9 figures of 1000 numbers. For this reason, if a number can be mapped with a suitable function in 0-1000 (a margin is seen actually and it takes about 1200), a reverse length table can be used. This is called hash function and a reverse length table that used a hash function is called hash table. There is just because it carried out division process of the number in size of arrangement as an easy hash function. When size of arrangement is set to 1201 now, it is

h(n) =n mod 1021 (operator that mod asks for a surplus).

Although it is reason to make into the contents of master [h (number)] = there is one problem. As an example, a number is 850604014, and although remainder divided by 1021 is 746, 746 may be not

much (hash value) in others. This is called collision. Although it is in processing when there is a collision variously, there is a method of using the next column, and the like as simple management. A hash method has the conspicuous feature that time and effort of search does not change even if registration and search are very efficient and its data volume increases. being also alike that it is not concerned but a hash method is seldom used in business has many people who do not learn a hash method, it carries out and hash on a memory is easy on a disk file, reasons of taking time and effort are recollected. Although the mentioned above hash function is dramatically simple, a device is required for a hash function by a character string (for example, name) to a slight degree. The following functions are used as hash of a character string.

**h=(... ((s [1] *37 + s [2]) *37 + s [3]) *37 ...) s[n] *37**

hash function is a function which makes «a random value» from a value of a key, there are an algorithm and relation of random number generation.

The above resembles well the random number generating method of a «linear congruential method». In other prominent random number generating methods can be used as a hash function. Since a hash function makes a value that does not overlap as much as possible from the original value, it has a case where a function similar to a hash function as «electronic fingerprints» that shows the feature of data is used.

In this case, by actual data, a function from which duplication cannot take place probably is devised by enlarging the range of function enough and devising a function. Electronic fingerprints are used when it is shown that data is not altered and they are important for electronic commerce technology. Since a hash function makes a random value from the original data, it may call a kind of encryp tion hash, and comes to nuance called hash exactly, but this is inaccurate direction for use. 1201 is a prime number, size of a table has a preferred prime number. Performance changes with capacity factors of a table. In the case of 80 percent of a capacity factor, it can refer also to the simplest method by about an average of three operations. Since efficiency will worsen if a hash table gets data blocked, when getting it blocked to some extent (example: 90% of capacity factor), size of a table is enlarged and data may be repacked. This is called re-hash. Hash is meaningful in «Chopping up» in English, and became the origin of a word of rice with hashed meat from hashed beef.

[010]

Operation of search is used very frequently in programming, when there is comparatively little target data volume, even if it investigates in order simply, speed which is not is obtained by the latest high-speed machine. Speed is dramatically important, when data volume needs to be becoming large or it is necessary to search frequently.

There is very much literature about search and detailed explanation is good to have literature seen. It is shown briefly that it is needed for making a realization program for the time being here.

What it happens to think as calling it linear search of first of all is this method, and finds a thing which wants to access data in an order from a head, and to look for it simply. Merits of this method are a point that may be scattering and a point that it can understand immediately easily and can be made. It is necessary to align data before search in binary search that comes out later. If a demerit has a thing which speed is a point late in many cases, and wants to look for it to a direction of a head of data, it is quick, but when the worst, all the data will be seen. Thus, a problem of speed becomes larger as there is much data volume. A function of the linear search lsearch() and lfind() is in a library of C.

A method that is the most popular among binary search programmers can perform high-speed search only by comparatively easy preparation compared with a previous linear search. Here, it sees from usage. As for binary search, data needs to be sorted by ascending order as conditions. Although this becomes a neck of this method in fact, data is co mparatively fixed, and it is good, when it sorts once, the rest repeats search and it is the mentioned above that it carries out.

However, since it must sort whenever data changes when both of change and addition of search and data are frequent, a phenomenon in which take time of sorting and it synthetic completely is not quick however quick search may be may also happen. It needs to be cautious of this point enough, sorting generally takes time rather than search. Since it searches by sensibility that a hit is attached and compared suitably (per middle) and per front middle will compare from it if larger than an object since data is sorted as structure, it is not necessary to see all the data. Data is sorted first, a comparison function used at this time and a comparison function used by search are meaningless if the same thing is not used. To sorted data, if found, the address will return. When not found, Null returns. When found, it is indicating how many of arrangement it is. It is convenient, when it is used for generally looking for an array of structures and the like, it refers to a member of a structure and it obtains an object. Since a result is obtained without seeing all the data, this retrieval system is a high speed compared with previous linearity search. Although sorting is a problem, and there are various algorithms also in sorting, quick sort generally used here is easy, and a high speed. However, when an omnipotent thing does not have sorting, either and it is characteristic along data of a basis, an algorithm that suited it should be used.

Point of quick sort sorted at high speed on the average without being comparatively dependent on distribution of data may be convenient, and it is used. In a hash search hash search, the search itself is a high speed overwhelmingly. When data is stored in a table as structure, a key is assigned by an easy formula, and data is stored in a place which can fly direct by the key. A key is calculated by same formula in the case of search, and it obtains the place direct. For example, what added all codes of the character string is a key to store a character string. Since a table for storing cannot usually be taken indefinitely, remainder that divided what was added altogether by the number of tables is used as an actual key. Since there is a possibility of enough that a key will overlap, in order to correspond to it, a method which makes a storage location arrangement form or has looked for a table vacant from the key enough in order, and carries out it is taken. A character string to store in a table is passed by an argument, and a key of a storage location returns. If the key is passed, a character string will return. A character string is passed, it investigates whether it exists in a table, and a key will be returned if it exists. If these are used, management becomes possible by making a character string into a numerical value, and a character string without length restrictions can be treated as an integer in a program. Since the only key is certainly assigned to a certain character string, comparison etc. can be performed with a value of the key.

A number of the array at the place by just because it added all character codes of a character string and broke by a size of an array is collectively used as a key. Once, 0 is using a value carried out +1, in order to use for an error judging. Thus, since it flies to a storage location only by calculating a key in a hash search, even if the number of anything of data increases, time of search does not change.

If the number of arrangement of a calculation place of the first key increases in the case of reverse search and registration, it will come to take time gradually, but if dispersibility is still improved by calculation of the first key, unless it inclines not much fatally, speed does not become slow so much. Although there is also an individual field that it is better not to carry out or management is difficult and deletion is also impossible, in a hash search, overwhelming strength is shown on coding of a character string that was especially described above. It is the optimal when registered contents do not need to be changed. The function hsearch() is prepared for a library of C, and there is also dissatisfaction, such as a point that only one can have a table. Although a loop is used in a place which calculates a key, the number of times of the loop there is reduced and improvement in the speed is possible too. Although a linear search binary search hash search was taken up here, there are still various algorithms, such as search using data of a tree structure.

Since there is no omnipotent thing, when high-speed search is needed, it is necessary to fully inquire from a data structure and to use the optimal search. In order to correspond to various search, various kinds of tables only for search have been prepared, but if time and effort that also updates a table for search collectively, and memory usage of the table itself are considered when data is updated, a method for post-installation is almost ineffective in many cases.

[011]

We will consider an attack concrete next. First, there is an attack of a kind generally called port scan (Port Scan) as an attack of the 1st kind by a cracker. Although this attack does not do direct damage to a network, it is used as an attack of that preceding paragraph story in many cases. In this attack, a cracker carries out repeating transmission of the IP packet from a host under own management to a network of a target of attack, changing suitably destination IP addresses and a destination port number in a packet. And a response to those IP packets is observed by the mentioned above host. This searches for an IP address and a port number that are used for communication with the exterior without receiving restriction by a fire wall in a network of a target of attack. Here, the mentioned above port number is data that expresses service kinds (for example, telnet, ftp, smtp, tftp and so on) of application software that operates on TCP or UDP, and is given to a TCP header or an UDP header in an IP packet. In this kind

of attack, transmission of the above IP packets, usually, it is carried out using exclusive use tool software, and destination IP addresses differ from a port number mutually to a network of a target of attack, and many IP packets whose transmitting agency IP address is the same are comparatively transmitted into a short time. Then, inside of a plurality of the mentioned above IP packets that acquired the mentioned above attack detection means and were held in this invention, they are a plurality of IP packets transmitted to the mentioned above network into predetermined time from the exterior, a transmitting former IP address is mutually the same at least, and, in more than a predetermined number, that from which destination IP addresses or a destination port number differs mutually detects that the mentioned above attack of the 1st kind was made at a certain time. Thus, an attack of the 1st kind called port scan is certainly detectable. Next, there is an attack of a kind generally called Syn-flood as an attack of the 2nd kind by a cracker. This attack brings down a specific host in a network using the characteristic of TCP. That is, in TCP, when communicating between 2 hosts, establishment processing of a logical connection is first performed among both hosts. In this connection establishment processing, an IP packet for Syn is transmitted from one host to a host of another side. This IP packet for Syn will be an IP packet that made the mentioned above one host's IP address, and an IP address of a host of another side a

transmitting agency IP address and destination IP addresses, respectively here, if it is the mentioned above in detail, only a Syn bit of a TCP header in the packet and a Syn bit of the Ack bits are set to «1».

And in connection establishment processing, a host of another side who received this IP packet for Syn transmits an IP packet for Syn/Ack to the mentioned above one host. Here this IP packet for Syn/Ack, in detail, it is the IP packet that made an IP address of a host of the mentioned above another side, and one host's IP address a transmitting agency IP address and destination IP addresses, respectively, and both Syn bits and Ack bits of a TCP header in the packet are set to «1». The mentioned above one host that received this IP packet for Syn/Ack in connection establishment processing, an IP packet for Ack is transmitted to a host of the mentioned above another side, and establishment of a logical connection between both hosts is made because a host of the mentioned above another side receives this IP packet for Ack. The the mentioned above Ack IP packet is an IP packet that has same transmitting agency IP address and destination IP addresses as the mentioned above IP packet for Syn in detail, and sets only a Syn bit of a TCP header in the packet, and an Ack bit of the Ack bits to «1».

[012]

The mentioned above Syn-flood is the attack using the characteristic of such TCP. In this attack, a cracker transmits many IP packets for Syn to within a

comparatively short time to a specific host of a network of a target of attack. And even if an IP packet for Syn/Ack is transmitted from the mentioned above specific host to each of those IP packets for Syn, an IP packet for Ack is not transmitted to the specific host.

When such an attack is made, the mentioned above specific host, after transmitting an IP packet for Syn/Ack to an IP packet for Syn transmitted first, predetermined time (generally 2 minutes) will be in a reception waiting state of the packet for Ack, unless a packet for Ack is transmitted to within the time. And whenever the new packet for Syn is transmitted in this state, the mentioned above specific host accumulates information on that new packet for Syn in a buffer space for communications processing that connection establishment processing according to the new packet for Syn should be completed in order. When there is a limit in a size of a buffer space and this buffer space fills, it becomes impossible however, for the mentioned above specific host to perform communications processing of TCP, and service processing on TCP. By this, a specific host will be downed. In this kind of attack (Syn-flood), comparatively many IP packets for Syn are transmitted to within the above comparatively short time to a specific host (host who has a specific IP address) in a network of a target of attack. According to this, many IP packets for Syn/Ack are transmitted to within a comparatively short time toward the network exterior from the specific host concerned.

A packet for Ack that should be eventually transmitted to the mentioned above specific host corresponding to those IP packets for Syn or an IP packet for Syn/Ack is not transmitted to the specific host. Next, inside of a plurality of the mentioned above IP packets that acquired the mentioned above attack detection means and were held in this invention, they are a plurality of IP packets for Syn based on TCP (Transmission Control Protocol) transmitted to the mentioned above network into predetermined time from the exterior, in more than a predetermined number, the same thing mutually at least the destination IP addresses and when it has same transmitting agency IP address and destination IP addresses as each of that IP packet for Syn and an IP packet for Ack based on the mentioned above TCP is not acquired in the mentioned above predetermined time, it detects that the mentioned above attack of the 2nd kind was made. Or inside of a plurality of of the mentioned above IP packets that acquired the mentioned above attack detection means and were held, they are a plurality of IP packets for Syn/Ack based on TCP (Transmission Control Protocol) transmitted to the exterior into predetermined time from the mentioned above network, in more than a predetermined number, the same thing mutually at least, respectively, a transmitting former IP address and when what is an IP packet for Ack based on the mentioned above TCP, and has the respectively same destination IP addresses as a transmitting agency IP

address of each of the mentioned above IP packet for Syn/Ack and destination IP addresses and a transmitting agency IP address is not acquired in the mentioned above predetermined time, it detects that the mentioned above attack of the 2nd kind was made. Thus, an attack of the 2nd kind called Syn-flood is certainly detectable.

Next, there is an attack of a kind generally called Teardrop as an attack of the 3rd kind by a cracker. This attack brings down a specific host in a network using the characteristic of processing according to separate control (what is called an IP fragment) of an IP packet. That is, an IP packet is a process in which an Internet top is transmitted via a router, and may be divided for administrative purposes on a relation of data processing capacity of each router. Since an error arises when an IP packet is transmitted in each router, in such a case, a router broadcasts an IP packet again. For this reason, in a host of destination IP addresses of an IP packet, some same IP packets divided for administrative purposes that it is received by more than one. Since it is such, in communication based on IP, when a received IP packet is divided for administrative purposes, a host (host of destination IP addresses) that receives an IP packet eventually does accumulation maintenance of the IP packet of each divided part until it receives an IP packet of all the remaining separate control portions. And after receiving an IP packet of all the separate control portions, processing which arranges them and restores

data of the original IP packet is performed. The mentioned above Teardrop is the attack using the characteristic of processing according to separate control of such an IP packet. In this attack, a cracker transmits an IP packet of the remaining separate control portion to that specific host, after transmitting an IP packet of many same separate control portions to a specific host of a network of a target of attack within a comparatively short time. When such an attack is made, the mentioned above specific host, when an IP packet of the remaining separate control portion is received eventually, in order to perform processing that is going to restore data of the original IP packet from the IP packet and an IP packet of a lot of divided parts transmitted previously, the processing takes a long time. For this reason, this specific host will be downed as a matter of fact. In this kind of attack (Teardrop), an IP packet of many same separate control portions is transmitted to a specific host in a network like the mentioned above within a comparatively short time. Then, inside of a plurality of the mentioned above IP packets which acquired the mentioned above attack detection means and were held in this invention, it is the divided IP packet of plurality transmitted to the mentioned above network into predetermined time from the exterior, and, in more than a predetermined number, the same divided part detects that the mentioned above attack of the 3rd kind is made at a certain time.

Thus, an attack of the 3rd kind called Teardrop is certainly detectable. Next, there is an attack of a kind generally called Land as an attack of the 4th kind by a cracker. This attack is an attack a transmitting agency IP address and whose destination IP addresses are the same and which transmits an impossible IP packet to a specific host of a network of a target of attack regularly. A specific host to whom such an IP packet was transmitted takes time in processing of the IP packet in many cases and it is often downed.

[013]

In this kind of attack, an IP packet with same transmitting agency IP address and destination IP addresses is transmitted to a specific host in a network like the above. And generally such an IP packet is transmitted to plurality and the mentioned above specific host within a comparatively short time. Next, inside of a plurality of the mentioned above IP packets that acquired the mentioned above attack detection means and were held in this invention, it is a plurality of IP packets transmitted to the mentioned above network into predetermined time from the exterior, and, in more than a predetermined number, that from which a transmitting former IP address is destination IP addresses and the same address detects that the mentioned above attack of the 4th kind is made at a certain time. Thus, an attack of Land and the 4th kind breaking is certainly detectable.

Generally an attack called Syn-flood, Teardrop and Land that were mentioned above belongs to an attack of a kind called DoS (Denial of Service). And this DoS includes an attack of a kind called Smurf other than Syn-flood, Teardrop, and Land, for example, an attack of a kind called Floodie and the like. Although Syn-flood, Teardrop and Land were typically mentioned as an attack of a kind belonging to DoS in this specification, it is also possible to detect an attack of Smurf, Floodie and so on. In this invention provided with an attack detection means to detect an attack by a cracker as mentioned above, processing that the mentioned above processing means performs is processing which generates a report and output showing the mentioned above attack having been detected, for example. By generating of this report and output, a network administrator or an external technician becomes possible taking a measure for eliminating a detected attack. Or processing that the mentioned above processing means performs is processing that carries out predetermined time inhibition of the penetration to the mentioned above network of an IP packet that has a specific transmitting agency IP address and/or destination IP addresses according to the mentioned above attack that the mentioned above attack detection means detected after detecting the mentioned above attack.

[014]

A hash method with time cue is used as a high-speed search algorithm. The concrete feature was shown on the following examples. On the other hand, kernel-coding of LINUX was adopted as a coding method. Thus, a function of OS was not used, but a program that carries out a direct interface and an exchange was produced. Although development will take this most time, a made soft speed became very high. Generally, exchanges with an interface are main work of OS, and the user of OS can receive offer as a subroutine to which an interface was attached in it. Next, for example, it was not opened to the usual UNIX (registered trademark) user, it becomes unnecessary to also have accessed memory management information, but since speed was thought as important, a code that carries out a direct drive was produced here. For the purpose of managing the various whole hardware environments efficiently, in order to specialize in a promising, but single function and to raise performance, the necessity of avoiding comes out of OS. In the conventional similar art, it became a low speed efficiently instead of the ability of development to be comparatively managed in a short time since the development so far is not performed. This time, it is the portion begun and developed in the world. If it is only mere detection, it is because it was unnecessary, because the rapidity so far was enough when it left record at the latest within time

(for example, 1 to 2 seconds) of a grade sufficiently early for human when it was seen from machinery. This time, since we needed to judge and intercept at time (about 1 / 1000 seconds) until a packet passes, we could not but prepare a high-speed algorithm and a high-speed program execution system. And a product that employed processing in full efficiently at high speed is done. In others, a function in which a table of a hash value changes with time exists. Information on an old packet is extinguished automatically. In order to oppose an attack of the Internet, and an attack that is called DoS especially as for it, the ability to respond to a certain amount of number of attack packets is needed for within the fixed time. A role that time cue plays is important. In too much a long time between each packet, since an offensive effect as DoS fades, setting out of elimination is needed.

[015]

[Embodiment of the invention] One embodiment of this invention is described with reference to drawing 1. Drawing 1 is a system configuration drawing of this embodiment. In drawing 1, 1 is LAN as a network. This LAN 1 is built, for example using Ethernet (registered trademark) and a plurality of hosts (computer) that omit a graphic display are connected via the Ethernet cable, a hub and the like. The Ethernet card that connects it to the Ethernet cable at each host, software for processing TCP/IP and various application software (for example, telnet, ftp, smtp, and so on) that functions on TCP/IP are mounted, and

communication based on IP is enabled. LAN 1 may be built with other embodiments, such as what not only was built on Ethernet, but a token ring. In the system of this embodiment, the computer 2 (this computer 2 is only next called the fire wall 2) that has the function of the fire wall as a packet filter is formed in the entrance of LAN 1. And LAN 1 is connected to the Internet 3 via the fire wall 2. The fire wall 2 has a file (next a filter configuration file) in which the data that specifies whether the penetration to LAN 1 of what kind of kind of IP packet is forbidden is written. And the fire wall 2 is this filter configuration file, when the IP packet of the kind to which the penetration to LAN 1 was forbidden has been transmitted from the Internet 3 side, discards that IP packet and prevents the penetration to LAN 1.

When the IP packet to which the penetration to LAN 1 is not forbidden has been transmitted by the filter configuration file, it is transmitted to LAN 1. The hub 4 is infixed between the fire wall 2 and the Internet 3, and the sensor 5 that has the function of the attack detection means is connected to this hub 4. The director 6 that has a function of a processing means to control the mentioned above fire wall 2 is connected to this sensor 5. These sensors 5 and directors 6 are constituted by the computer, respectively. The mentioned above sensor 5 is constituted by the UNIX machine and connected to the mentioned above hub 4 by the Ethernet card 7.

In this case, software called tcpdump is mounted in the sensor 5. By this tcpdump, all IP packets that pass along the hub 4 are acquirable via the Ethernet card 7 (a hearing is carried out). Such operation is called promise cast mode in many cases. And the sensor 5 is made to carry out the hold stores of each acquired IP packet to the hard disk that is not represented with the time information at the acquisition time. When the total amount of the IP packet which carried out hold stores to the hard disk reaches a predetermined permissible dose, the sensor 5 eliminates the oldest IP packet and carries out the hold stores of the newly acquired IP packet to a hard disk. The sensor 5 does not have an IP address, but ARP ( Address Resolution Protocol), even if packets to which a response is urged, such as a packet of RARP (Reverse Address Resolution Protocol), are transmitted, it is set up by software not carry out the response to it.

That is, the sensor 5 performs only reception (incorporation) of an IP packet and can carry out software (following and attack detection algorithm) for detecting the attack of the 1st - the 6th kind that were mentioned above is mounted in the sensor 5. This attack detection algorithm is mounted in the director 6, and it may be made to make this attack detection algorithm process in the sensor 5, performing data transfer with this director 6. Software (next a filter control algorithm) that controls the mentioned above fire wall 2 is mounted in the mentioned above director 6.

In this case, according to the attack detected by the sensor 5, a filter control algorithm is rewriting the data of the mentioned above filter configuration file suitably and controls the mentioned above fire wall 2.

[016]

Next, the operation of this embodiment of this is explained. The mentioned above sensor 5 performs the following processings for every predetermined cycle time, carrying out the hold stores of the IP packet acquired to a hard disk like the mentioned above. That is, after classifying a plurality of IP packets for a predetermined time interval according to the value of a transmitting agency IP address and destination IP addresses from a hard disk, the sensor 5 is incorporated into the memory that is not represented and is held. That is, put together what has the same transmitting agency IP address among a plurality of IP packets for a predetermined time interval, and a thing with the same destination IP addresses is put together, and it incorporates into a memory (in the following explanation, the group of the IP packet put together in this way is called IP packet group). And after processing the attack detection mentioned later to a plurality of IP packets incorporated into this memory, those IP packets are eliminated from a memory. In this case, in each cycle time, the IP packet incorporated into a memory is acquired from the acquisition times of the oldest IP packet of the IP packets incorporated into the memory in the last cycle time after the time which went

through predetermined time. Processing of the attack detection by the sensor 5 in each cycle time is performed as follows according to an attack detection algorithm. The sensor 5 delivers first an attack of the 1st kind, namely, the processing which detects port scan, the mentioned above 1st- 6th among the attacks of the kind. A transmitting agency IP address is the same among the IP packets that incorporated the sensor 5 into the memory as mentioned above in this processing, and the value (this is a value of the IP address belonging to LAN 1) of all the destination IP addresses which the IP packet by which this transmitting agency IP address is included in each of that IP packet group to each IP packet group which is a thing of the exterior of LAN 1 has is extracted. And each value of the destination IP addresses extracted by each of the mentioned above IP packet groups is received from the IP packet group (IP packet group of the same transmitting agency IP address). The number of the IP packet which it has the same destination IP addresses as the value of these destination IP addresses, and the destination port numbers in a TCP header or an UDP header differed mutually and was acquired in the continuous predetermined time (for example, inside of 30 seconds) is counted. When this count number reaches a predetermined number (for example, 20 pieces) at this time, the sensor 5 detects that the attack of port scan is made.

And the data in which that is shown, and the value data of the transmitting agency IP address of the IP packet group as which this attack was detected are given to the mentioned above (these data is next called 1st kind attack detection data) director 6. Such processing has the same transmitting agency IP address, and this transmitting agency IP address is performed one by one to all the IP packet groups that do not belong to LAN 1. Although the port number counted the number of a mutually different IP packet in detection of the port scan in this embodiment, it may be made to detect port scan by the following processings. That is, a transmitting agency IP address is the same, and the value of all the destination port numbers which the IP packet contained in each of that IP packet group has is extracted to each IP packet group in which this transmitting agency IP address is a thing of the LAN 1 exterior. To each value of the extracted destination port number from the IP packet group which extracted this destination port number. The number of the IP packet that it has the same destination port number as the value of this destination port number, and destination IP addresses differed mutually and was acquired in the continuous predetermined time is counted. And when the count number reaches a predetermined number, it detects that port scan is performed. On the other hand, the mentioned above director 6 that was able to give the above 1st kind attack detection data from the sensor 5,

the filter configuration file of the mentioned above fire wall 2 is rewritten so that predetermined time (for example, for 5 minutes) inhibition of the IP packet that has the same transmitting agency IP address as the transmitting agency IP address included in this 1st kind attack detection data advancing into LAN 1 may be carried out from the present. If the IP packet in which the fire wall 2 has the mentioned above transmitting agency IP address at this time is transmitted from the Internet 3, that IP packet will be discarded and the penetration to LAN 1 will be prevented. Thus, LAN 1 is protected from the attack of port scan. By the time the mentioned above predetermined time (for 5 minutes) passes, the director 6, if the same 1st kind attack detection data as the 1st kind attack detection data given previously is again given from the sensor 5, the fire wall 2 is controlled to prevent the penetration to LAN 1 of the IP packet from the transmitting agency IP address of the mentioned above predetermined time (for 5 minutes) and this 1st kind attack detection data from the point in time. Thus, as long as the attack of port scan continues, the IP packet from a transmitting former IP address cannot advance into LAN 1.

And the director 6 cancels inhibition of the penetration to LAN 1 of the IP packet from the transmitting agency IP address of the 1st kind attack detection data, when the mentioned above 1st kind attack detection data is not given, by the time the

mentioned above predetermined time (for 5 minutes) passes. The sensor 5 that performed detection processing of the attack of port scan as mentioned above performs detection processing of an attack (Syn-flood) of the 2nd kind next.

[017]

In this processing, the sensor 5 extracts the IP packet for Syn by which destination IP addresses are included in this IP packet group to each IP packet group of the destination IP addresses that belong to LAN 1 among the same IP packet groups one by one in order of those acquisition times. and extracted every IP packet for Syn acquired from the acquisition times of the IP packet for Syn in predetermined time (for example, for 2 seconds) investigates whether it exists in the IP packet group of the same destination IP addresses. And when such an IP packet for Syn exists, the number of those IP packets for Syn including the IP packet for Syn extracted previously is counted. Each of the counted IP packet for Syn is received, the IP packet for Ack corresponding to each (the same detailed transmitting agency IP address as this IP packet for Syn) and it is an IP packet for Ack that has the next sequence number of the sequence number in the TCP header of this IP packet for Syn, and what was acquired from the acquisition times of this IP packet for Syn in the mentioned above predetermined time (for 2 seconds) investigates whether it exists in the IP packet group of the same destination IP addresses.

When such an IP packet for Ack exists at this time, the mentioned above count number is decreased by «1» every each time. And when finishing investigating existence of the corresponding IP packet for Ack eventually and the mentioned above count number is more than a pred etermined number (for example, 16 pieces). The data that detects that the attack of Syn-flood is made and in which that is shown, the value data of the transmitting agency IP address of the IP packet for Syn as which this attack was detected, and the value data of destination IP addresses are given to the mentioned above (these data is next called 2nd kind attack detection data) director 6. Such processing has the same destination IP addresses, and these destination IP addresses are performed one by one to all IP packet groups belonging to LAN 1. Although Syn-flood was detected based on the number of the IP packet for Syn, it may be made to detect Syn-flood by the following processings in this embodiment.

That is, a transmitting agency IP address is the same, and the IP packet for Syn/Ack contained in this IP packet group is extracted one by one in order of the acquisition times to each IP packet group to which this transmitting agency IP address belongs to LAN 1. And extracted every IP packet for Syn/Ack acquired from the acquisition times of the IP packet for Syn/Ack in predetermined time (for example, for 2 seconds) investigates whether it exists in the IP packet group of the same transmitting agency IP address.

When such an IP packet for Syn/Ack exists at this time, the number of those IP packets for Syn/Ack including the IP packet for Syn/Ack extracted previously is counted. The IP packet group of the same destination IP addresses as the transmitting agency IP address of this IP packet for Syn/Ack is investigated to each of the counted IP packet for Syn/Ack. The IP packet for Ack corresponding to this IP packet for Syn/Ack at this time (the same detailed destination IP addresses as the transmitting agency IP address of this IP packet for Syn/Ack) and it is an IP packet for Ack that has the next Ack number of the sequence number in the TCP header of this IP packet for Syn/Ack, and what was acquired from the acquisition times of this IP packet for Syn/Ack in the mentioned above predetermined time (for 2 seconds) investigates whether it exists in the IP packet group concerned. And when such a packet for Ack exists, the mentioned above count number is decreased by «1» every each time. And when finishing investigating existence of the corresponding IP packet for Ack eventually and the mentioned above count number is more than a predetermined number (for example, 16 pieces), it detects that the attack of Syn-flood is made.

[018]

The data given to the director 6 from the sensor 5 in this case is data in which hav ing detected the attack of Syn-flood is shown, value data of the transmitting agency IP address of the mentioned above IP packet

for Syn/Ack, and value data of destination IP addresses. In this case, the value data of the transmitting agency IP address of the IP packet for Syn/Ack and the value data of destination IP addresses, respectively, it is equivalent to the value data of the IP packet destination IP addresses for Syn in the mentioned above 2nd kind attack detection data explained previously and the value data of a transmitting agency IP address. On the other hand, the mentioned above director 6 that was able to give the above 2nd kind attack detection data from the sensor 5, the filter configuration file of the mentioned above fire wall 2 is rewritten, so that predetermined time (for example, for 2 minutes) inhibition of the IP packet that has the same transmitting agency IP address as the transmitting agency IP address included in this 2nd kind attack detection data advancing into LAN 1 may be carried out from the present. Simultaneously, the director 6 rewrites the filter configuration file of the fire wall 2 so that predetermined time (for example, for 2 seconds) inhibition of the IP packet that has the same destination IP addresses as the destination IP addresses included in the 2nd kind attack detection data advancing into LAN 1 may be carried out from the present. If the IP packet in which the fire wall 2 has the mentioned above transmitting agency IP address at this time or the IP packet that has the mentioned above destination IP addresses is transmitted from the Internet 3,

that IP packet will be discarded and the penetration to LAN 1 will be prevented. Thus, LAN 1 is protected from the attack of Syn-flood, and it can return to an all seems well, without downing the host of the IP address made into the object of this attack.

Like the case at the time of detection of port scan, the director 6, by the time the mentioned above predetermined time (for 2 minutes) according to exclusion of the IP packet which has a transmitting agency IP address in the 2nd kind attack detection data passes, if the same 2nd kind attack detection data as the 2nd kind attack detection data given previously is again given from the sensor 5, the fire wall 2 is controlled to prevent the penetration to LAN 1 of the IP packet from the transmitting agency IP address of the mentioned above predetermined time (for 2 minutes) and this 2nd kind attack detection data from the point in time. This is the same also about exclusion of the IP packet which has the destination IP addresses in the 2nd kind attack detection data. Thus, as long as the attack of Syn-flood continues, the IP packet from the transmitting agency IP address according to the attack or the IP packet to the destination IP addresses according to the attack cannot advance into LAN 1. And the director 6 about all of exclusion of the IP packet that has a transmitting agency IP address in the 2nd kind attack detection data and exclusion of the IP packet which has the destination IP addresses in the 2nd kind attack detection data.

By the time the mentioned above predetermined time (for 2 minutes, for 2 seconds) corresponding to each passes, when the mentioned above 2nd kind attack detection data is not given, inhibition of th e penetration to LAN 1 of the IP packet that has a transmitting agency IP address of the 2nd kind attack detection data or the IP packet that has destination IP addresses of the 2nd kind attack detection data is canceled. The sensor 5 which performed detection processing of the attack of Syn-flood as mentioned above performs detection processing of an attack (Teardrop) of the 3rd kind next. In this processing, the sensor 5 extracts the IP packet (only next a separate control packet) by which destination IP addresses are included in this IP packet group to each IP packet group of the destination IP addresses that belong to LAN 1 among the same IP packet groups and which was divided for administrative purposes one by one. In this case, in IP, the specific flag in that IP header is «1» or the separate control packet serves as a value with bigger data called fragmentation offset than «0». Thus, a separate control packet can be found out and the sensor 5 is acquired from the acquisition times of each extracted separate control packet in predetermined time (for example, for 5 minutes), and what has respectively same IP identification number in this separate control packet and an IP header and value of fragmentation offset

(the same separate control packet as the extracted separate control packet) investigates whether it is in the same IP packet group as this separate control packet. When there is such a separate control packet at this time, the number of those separate control packets including the separate control packet extracted previously is counted.

And when this count number is more than a predetermined number (for example, 80 pieces), it detects that the attack of Teardrop is made and the data in which that is shown and the value data of the transmitting agency IP address of the separate control packet as which this attack was detected and the value data of destination IP addresses are given to the mentioned above director 6 (these data is next called 3rd kind attack detection data). Such processing has the same destination IP addresses, and these destination IP addresses are performed one by one to all the IP packet groups belonging to LAN 1.

On the other hand, the mentioned above director 6 that was able to give the above 3rd kind attack detection data from the sensor 5 does firewall control in the completely same way as the case where the mentioned above Syn-flood is detected. That is, the filter configuration file of the mentioned above fire wall 2 is rewritten, so that predetermined time (for 2 minutes) inhibition of the IP packet which has the same transmitting agency IP address as the

transmitting agency IP address included in the 3rd kind attack detection data advancing into LAN 1 may be carried out from the present. The filter configuration file of the fire wall 2 is rewritten so that predetermined time (for 2 seconds) inhibition of the IP packet that has simultaneously the same destination IP addresses as the destination IP addresses included in the 3rd kind attack detection data advancing into LAN 1 may be carried out from the present.

Thus, LAN 1 is protected from the attack of Teardrop and it can return to an all seems well, without downing the host of the IP address made into the object of this attack.

[019]

The sensor 5 that performed detection processing of the attack of Teardrop as mentioned above performs detection processing of an attack (Land) of the 4th kind next. In this processing, the sensor 5 extracts the IP packet which has a transmitting agency IP address of the same value as the destination IP addresses of each IP packet group to this IP packet group of the destination IP addresses that belong to LAN 1 among IP packet groups with same destination IP addresses. It is investigated whether the IP packet that has the same transmitting agency IP address as this IP packet, and was acquired from the acquisition times of this IP packet in predetermined time (for example, for 2 minutes) exists out of the IP packet group of the same destination IP addresses as the extracted IP packet.

And when such an IP packet exists, the number of this IP packet of those IP packets including the IP packet extracted previously is counted. When this count number is more than a predetermined number (for example, 6 pieces) at this time, it detects that the attack of Land is made and the data in which that is shown, and the value data of the transmitting agency IP address of the IP packet as which this attack was detected are given to the mentioned above (these data is next called 4th kind attack detection data) director 6. Such processing has the same destination IP addresses, and these destination IP addresses are performed one by one to all the IP packet groups belonging to LAN 1. On the other hand, the mentioned above director 6 that was able to give the above 4th kind attack detection data from the sensor 5, it has the same transmitting agency IP address as the transmitting agency IP address included in the 4th kind attack detection data, and the filter configuration file of the mentioned above fire wall 2 is rewritten so that predetermined time (for example, for 3 minutes) inhibition of the IP packet that has the same destination IP addresses as this transmitting agency IP address advancing into LAN 1 may be carried out from the present. If the IP packet in which the fire wall 2 has the mentioned above transmitting agency IP address and destination IP addresses at this time is transmitted from the Internet 3, that IP packet will be discarded and the penetration to LAN 1 will be prevented.

Thus, LAN 1 is protected from the attack of Land. In this case, like the case at the time of detection of port scan the director 6, by the time the mentioned above predetermined time (for 6 minutes) according to exclusion of the IP packet that has the same transmitting agency IP address and destination IP addresses as the transmitting agency IP address in the 4th kind attack detection data passes, if the same 4th kind attack detection data as the 4th kind attack detection data given previously is again given from the sensor 5, the fire wall 2 is controlled to prevent the penetration to LAN 1 of the IP packet that has the transmitting agency IP address and destination IP addresses of the mentioned above predetermined time (for 6 minutes), and this 4th kind attack detection data from the time. Thus, as long as the attack of Land continues, the IP packet that has the transmitting agency IP address and destination IP addresses according to the attack cannot advance into LAN 1. And by the time the mentioned above predetermined time (for 6 minutes) passes, when the mentioned above 4th kind attack detection data is not given, the director 6. Inhibition of the penetration to the same transmitting agency IP address as the transmitting agency IP address of the 4th kind attack detection data and LAN 1 of an IP packet that carry out a destination IP addresses owner is canceled. Although the value data of the transmitting agency IP address of the IP packet according to the attack of Land was given to

the director 6 as 4th kind attack detection data in this embodiment, the transmitting agency IP address of the IP packet according to the attack of Land and destination IP addresses are the same values. Thus, of course, the value of destination IP addresses may be given to the director 6 instead of the value data of a transmitting former IP address. As mentioned above, the sensor 5 that performed detection processing of the attack of Land performs processing that detects the attack (acquisition of a password) of the 5th kind next. In this processing, the sensor 5 extracts the IP packet in which destination IP addresses contain LAN 1's the user name data and pass word data of a host to each IP packet group of the destination IP addresses that belong to LAN 1 among the same IP packet groups. The number of the IP packet that user name data was the same and pass word data differed mutually, and was acquired in the continuous predetermined time (for example, for 2 minutes) out of those extracted IP packets is counted. If this count number is more than a predetermined number (for example, 20 pieces) at this time, the data that detects that the attack of the 5th kind for a cracker to gain a password is made and in which that is shown, the value data of the transmitting agency IP address of the IP packet as which this attack was detected, and the value data of destination IP addresses are given to the mentioned above (these data is next called 5th kind attack detection data) director 6.

Such processing has the same destination IP addresses, and these destination IP addresses are performed one by one to all the IP packet groups belonging to LAN 1. On the other hand, the mentioned above director 6 that was able to give the above 5th kind attack detection data from the sensor 5, the transmitting agency IP address of this 5th kind attack detection data. And the filter configuration file of the mentioned above fire wall 2 is rewritten, so that predetermined time (for example, 1 hour) inhibition of the IP packet that has the respectively same transmitting agency IP address and destination IP addresses as destination IP addresses advancing into LAN 1 may be carried out from the present. If the IP packet in which the fire wall 2 has the mentioned above transmitting agency IP address and an IP address at this time is transmitted from the Internet 3, that IP packet will be discarded and the penetration to LAN 1 will be prevented. Thus, LAN 1 is protected from the attack of the 5th kind that aimed at acquisition of the password.

[020]

Like the case at the time of detection of port scan, the director 6, by the time the mentioned above predetermined time (1 hour) according to exclusion of the IP packet which has the transmitting agency IP address and destination IP addresses in the 5th kind attack detection data passes, if the same 5th kind attack detection data as the 5th kind attack detection

data given previously is again given from the sensor 5, the fire wall 2 is controlled to prevent the penetration to LAN 1 of the IP packet that has the transmitting agency IP address and destination IP addresses of the mentioned above predetermined time (1 hour) and this 5th kind attack detection data from the time. Thus, as long as the attack of the 5th kind continues, the IP packet that has the transmitting agency IP address and destination IP addresses according to the attack cannot advance into LAN 1. And the director 6 cancels inhibition of the penetration to LAN 1 of the IP packet which has the transmitting agency IP address and destination IP addresses of the 5th kind attack detection data, when the mentioned above 5th kind attack detection data is not given, by the time the mentioned above predetermined time (1 hour) passes. As mentioned above, the sensor 5 which performed detection processing of the attack of the 5th kind performs processing that detects the attack (attack of a security hole) of the 6th kind next.

The sensor 5 has «Ipr» that is a logical name of a printer as opposed to each IP packet group of the destination IP addresses that belong to LAN 1 among IP packet groups with same destination IP addresses, and searches with this processing the IP packet whose data size is 128 or more characters. And when such an IP packet is found, the data that detects that the attack of the 6th kind that attacks the through hole of the host of LAN 1 is made and in which that is shown,

the value data of the transmitting agency IP address of the IP packet as which this attack was detected, and the value data of destination IP addresses are given to the mentioned above (these data is next called 6th kind attack detection data) director 6. On the other hand, the mentioned above director 6 that was able to give the above 6th kind attack detection data from the sensor 5, the transmitting agency IP address of this 6th kind attack detection data. And the filter configuration file of the mentioned above fire wall 2 is rewritten, so that predetermined time (for example, 4 hours) inhibition of the IP packet that has the respectively same transmitting agency IP address and destination IP addresses as destination IP addresses advancing into LAN 1 may be carried out from the present. If the IP packet in which the fire wall 2 has the mentioned above transmitting agency IP address and an IP address at this time is transmitted from the Internet 3, that IP packet will be discarded and the penetration to LAN 1 will be prevented. Thus, LAN 1 is protected from the attack of the 6th kind that attacks the through hole of the host of LAN 1.

Like the case at the time of detection of port scan, the director 6, by the time the mentioned above predetermined time (4 hours) according to exclusion of the IP packet that has the transmitting agency IP address and destination IP addresses in the 6th kind attack detection data passes, if the same 5th kind attack detection data as the 6th kind attack detection data given previously is again given from the sensor

5, the fire wall 2 is controlled to prevent the penetration to LAN 1 of the IP packet that has the transmitting agency IP address and destination IP addresses of the mentioned above predetermined time (4 hours) and this 6th kind attack detection data from the time. Thus, as long as the attack of the 6th kind continues, the IP packet which has the transmitting agency IP address and destination IP addresses according to the attack cannot advance into LAN 1. And the director 6 cancels inhibition of the penetration to LAN 1 of the IP packet IP packet which has the transmitting agency IP address and destination IP addresses of the 5th kind attack detection data, when the mentioned above 6th kind attack detection data is not given, by the time the mentioned above predetermined time (4 hours) passes. As it explained above, according to the system of this embodiment, the proper measures that protect LAN 1 from the detected attack can be automatically taken promptly the sensor 5 and only by introducing the director 6, detecting various kinds of attacks to LAN 1 by a cracker in real time.

For this reason, the labors which build LAN 1 in consideration of the attack by a cracker or refer to a log file frequently are reduced substantially and network administrators can reduce the cost of the control of maintenance of LAN 1 by extension. Since the various attacks by a cracker are detectable in real time, in the situation where an attack is not detected,

the necessity of restricting communication with LAN 1 and the exterior exceptionally decreases. For this reason, the flexibility of communication of LAN 1 can be raised at the time and it can usually utilize the information resource on the Internet 3 useful. In the embodiment described above, the fire wall 3 was formed in the entrance of LAN 1, and the attack by a cracker was detected, it solved, and treatment that eliminates the detected attack automatically by controlling this fire wall 3 was performed. However, when the attack by a cracker is detected, it may only be made to perform information to that effect to a network administrator, a special defense administrator, etc. In this case, the mentioned above director 6 or the sensor 5 is connected to hosts, such as a network administrator and a defense administrator, via the public line or the dedicated line, for example. And when an attack is detected, information like the 1st - 6th kind attack detection data mentioned above is transmitted to hosts, such as a network administrator and a defense administrator, from the director 6 or the sensor 5.

When it does in this way, a network administrator will perform directly concrete treatment for protecting LAN 1 from the detected attack. However, since what is necessary is just to take a measure when network administrators receive the mentioned above information, even if it is in this case and an offensive kind is also detected, the measures against an attack can be taken comparatively easily.

Although the mentioned above embodiment showed what detects the attack of the 1st - 6th kind in order, it is also possible for it to be made to perform detection processing of those attacks in parallel. The mentioned above embodiment showed what detects Syn-flood, Teardrop and Land among the attacks belonging to DoS (Denial of Service) mentioned above. However, in addition, it is also possible to detect an attack, such as DDoS(Distributed Denial of Service) Smurf and Floodie.

[021]

Industrial applicability

The cracker monitor system according to this invention as mentioned above, it is useful as a system that can be performed without protecting simply networks, such as LAN built by the organization of a company, a government office, and the like, from the attack by a cracker and spoiling the flexibility of communication by the protection more than needed.

## [Brief description of the drawings]

[Drawing 1] Drawing 1 is a system configuration drawing of one embodiment of the cracker monitor system according to this invention.

Drawing 1